CA Client Automation

Manuel d'implémentation

12.9



Produits CA Technologies référencés

Ce document contient des références aux produits CA suivants :

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA Asset Portfolio Management (CA APM)
- CA Business Intelligence
- CA Common Services™
- CA Desktop Migration Manager (CA DMM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Mobile Device Management (CA MDM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Process Automation
- CA Service Desk Manager
- CA WorldView™

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 2: Planification de l'implémentation d'infrastructure 79

Chapitre 3: Installation de Client Automation 111

Chapitre 4: Tâches post-installation 217

Chapitre 5: Déploiement de l'infrastructure 247

Chapitre 6: Remarques sur la migration et la mise à niveau 273

Chapitre 11: Fonctionnalités de sécurité Client Automation 407

Chapitre 12: Connectivité du réseau étendu (ENC) 467

Chapitre 14: Dépannage 529

Annexe A: Fichier de configuration du service d'automatisation 545

Annexe B: Ports utilisés par CA Client Automation 553

Annexe C: Procédures Software Delivery pour l'installation 571

Annexe D: Certificats actuels fournis par CA Client Automation 583

Annexe E: Cas d'utilisation de la prise en charge des zones de sécurité 589

Chapitre 1: Description de Client Automation

CA Client Automation est une solution de gestion d'actifs informatiques multiplates-formes qui fournit les fonctions Asset Management, Software Delivery et Remote Control pour toutes les entreprises.

Ce chapitre traite des sujets suivants :

Architecture DSM

CA Client Automation inclut une interface et une architecture communes pour les fonctions Asset Management, Software Delivery et Remote Control (architecture DSM), mais l'intégration est plus approfondie que l'interface utilisateur d'administration.

Les éléments essentiels de l'infrastructure sont partagés entre les fonctions et composants Asset Management, Software Delivery et Remote Control. Par exemple, la base de données de gestion, les communications, le contrôle de processus, la journalisation, la gestion des événements, etc. sont identiques, que vous installiez deux ou toutes les fonctions. Il en résulte des fonctionnalités utiles et une terminologie, une architecture, une interface et des données cohérentes entre toutes les fonctions installées.

En outre, l'architecture DSM présente un ensemble de concepts cohérents et communs qui sont également partagés par les fonctions Asset Management, Software Delivery et Remote Control. Ces composants partagés comprennent les éléments suivants :

- Interface utilisateur graphique (IUG)
- Gestionnaire
- Serveur de modularité
- Agent

L'architecture DSM est composée de plusieurs niveaux :

Console Web/Explorateur DSM

Permettent le contrôle administratif de Client Automation et de ses modules d'extension. L'explorateur DSM constitue l'interface utilisateur graphique pour Windows, tandis que la console Web est une IUG basée sur un navigateur pour Windows et Linux.

Gestionnaire d'entreprise

Fournit un point d'administration unique pour plusieurs domaines.

Gestionnaire de domaines

Fournit tous les services de gestion aux niveaux et agents inférieurs.

Serveur de modularité.

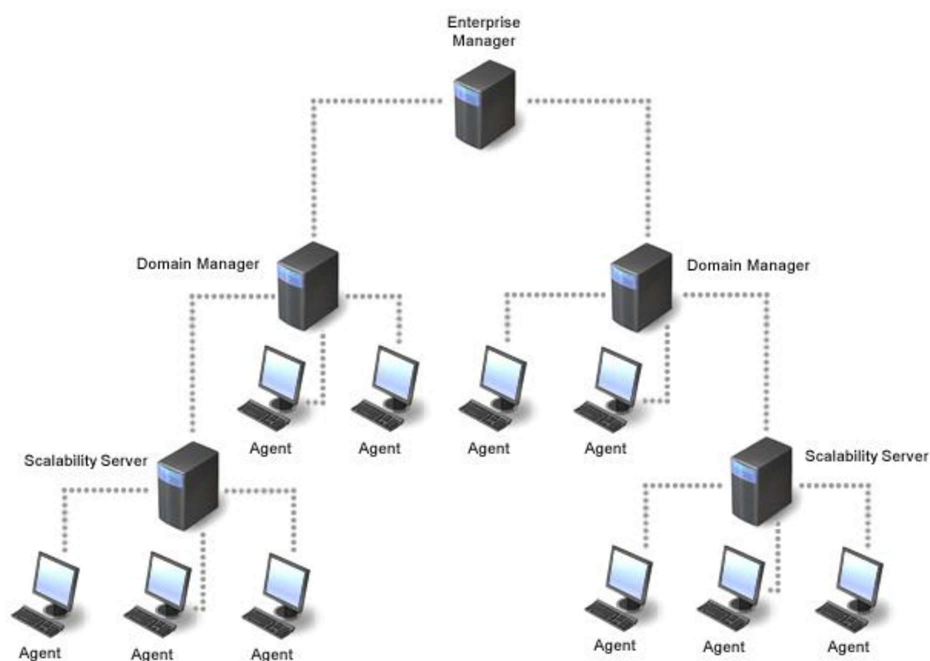
Sert de point de distribution pour Software Delivery et les activités de distribution et de point de collecte pour l'inventaire des actifs.

Agent

Fournit des services de contrôle distant, de livraison de logiciels et d'inventaire des actifs sur les hôtes pris en charge.

Chaque niveau du gestionnaire héberge une instance de la base de données de gestion (MDB).

Le schéma suivant illustre l'architecture à plusieurs niveaux. Dans cet exemple, un gestionnaire d'entreprise sert de point d'administration pour deux gestionnaires de domaine gérant chacun directement les agents connectés et un serveur de modularité en aval. Les serveurs de modularité gèrent les tâches entre les niveaux agent et gestionnaire de domaine.



Explorateur DSM

L'explorateur DSM constitue l'interface d'administration principale de Client Automation. Il est disponible dans les environnements d'exploitation Windows.

La barre de l'explorateur DSM située à gauche propose quatre types de vues différentes : Arborescence, Historique, Signets et Recherche. La vue Arborescence représente le mode d'affichage par défaut, qui constitue l'accès principal aux différentes fonctions de l'explorateur DSM.

Lorsque vous les sélectionnez dans la vue arborescente, de nombreux nœuds d'arborescence fournissent des listes affichées dans le volet droit.

De nombreux nœuds d'arborescence offrent également une présentation graphique de type Web. Le portail principal en est un exemple. Il fournit une présentation de Client Automation à l'échelle du système grâce à quatre portlets :

Fonctions principales

Permet d'accéder aux principales zones de l'explorateur DSM, telles que Ordinateurs et utilisateurs, Logiciel, Jobs etc.

Fréquemment utilisé

Donne accès aux nœuds de l'arborescence les plus fréquentés.

Etat du système

Affiche les informations sur le domaine connecté, telles que les statistiques, les échecs, les violations et les tâches en cours.

Démarrage rapide

Fournit un accès rapide aux fonctions les plus utilisées.

Vous pouvez personnaliser les portlets Etat du système et Démarrage rapide selon vos besoins.

Un didacticiel est accessible dans le volet droit de l'explorateur DSM. Il présente des informations sur la navigation dans l'explorateur DSM et des informations de mise en route concernant les tâches les plus courantes. Vous pouvez activer ou désactiver ce didacticiel en utilisant la fonction Barre du didacticiel accessible dans le menu Afficher de l'explorateur DSM.

Pour plus d'informations et une aide contextuelle, consultez l'*aide de l'explorateur DSM*.

Gestionnaire

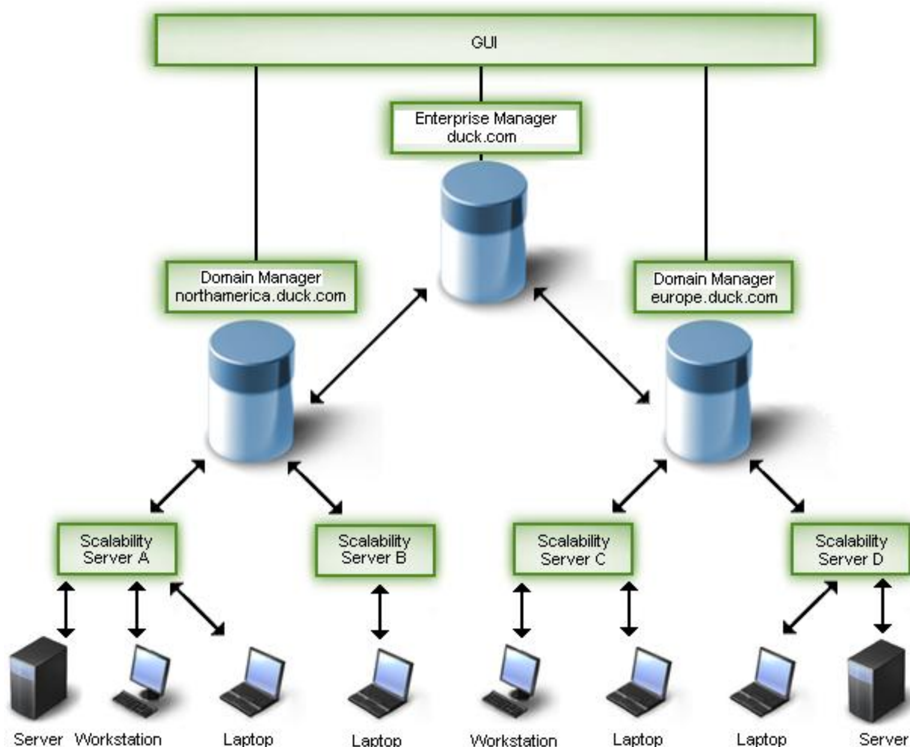
Les aspects suivants du rôle de gestionnaire dans Client Automation sont pris en considération :

- Concept Entreprise et domaine (page 25)
- Composants d'entreprise et de domaine (page 26)
- Concept Moteur (page 29)

Concept Entreprise et domaine

Client Automation dispose de deux niveaux de gestion, Domaine et Entreprise, pour lesquels des bases de données de gestion existent. Lorsque plusieurs domaines sont déployés au sein d'une organisation, Enterprise peut être déployé pour fournir un point de gestion unique.

L'illustration suivante présente un exemple d'architecture à deux niveaux composée du gestionnaire d'entreprise et des deux gestionnaires de domaines de la société, auxquels deux serveurs de modularité sont connectés :



Le gestionnaire d'entreprise, appelé duck.com, et les deux gestionnaires de domaine, l'un dédié à la gestion des tâches et unités en Amérique du Nord (northamerica.duck.com) et l'autre dédié à la gestion des tâches et unités en Europe (europe.duck.com). Deux serveurs de modularité sont connectés à chacun des gestionnaires de domaine afin de réduire leur charge de travail en gérant les unités des utilisateurs finaux tels que ordinateurs portables, stations de travail et serveurs supplémentaires.

Composants d'entreprise et de domaine

Voici une liste de termes et de définitions permettant de mieux comprendre le concept d'entreprise et de domaine de CA Client Automation.

Gestionnaire d'entreprise

Un *gestionnaire d'entreprise DSM* est un niveau de gestion supérieur facultatif pour CA Client Automation. Il fournit un point de gestion unique pour un groupe de domaines DSM. Il permet également de définir des configurations et des stratégies pour des groupes d'objets situés dans un ou plusieurs domaines. Il ne doit y avoir qu'un seul gestionnaire d'entreprise dans un environnement DSM.

Gestionnaire de domaines

Un *gestionnaire de domaine DSM* constitue le point central de gestion pour les autres composants DSM, notamment les serveurs de modularité et les agents.

Serveur de modularité.

Un *serveur de modularité DSM* représente un processus réparti formant l'interface principale pour l'agent. Les serveurs de modularité sont chargés de répartir la charge de travail DSM sur de nombreux hôtes.

Moteur

Un *moteur DSM* est un processus qui offre des services de communication entre les serveurs de modularité d'une part et leur domaine DSM parent et les gestionnaires d'entreprise d'autre part.

La base de données de gestion dans le concept Entreprise et Domaine

Les suites de produits CA Technologies sont intégrées grâce à un référentiel de données d'entreprise commun, la base de données de gestion (MDB). La MDB fournit une structure unifiée pour le stockage des données de gestion de tous les produits CA Technologies. La MDB intègre les données de gestion de toutes les disciplines informatiques et de tous les produits CA Technologies. Nos clients et partenaires extérieurs peuvent élargir la MDB pour inclure d'autres données de gestion informatique provenant d'outils et de produits logiciels tiers.

CA IT Client Manager se base sur MDB r1.5 SP1, qui installe par défaut uniquement les schémas DSM et d'actifs communs. Si un autre produit CA utilise la MDB créée par CA ITCM et s'il prend également en charge la MDB r1.5, ce produit doit alors installer son propre schéma sur la MDB existante.

Toutefois, si un produit CA prend en charge uniquement la MDB r1.0.4, l'installation échoue. Dans ce cas, installez la MDB avec l'option Mode de compatibilité activée. CA ITCM installe tout d'abord les patchs MDB r1.0.4 les plus récents, puis la MDB est mise à niveau vers MDB r1.5. Toutes les définitions de schémas sont donc présentes et seules les définitions de schémas DSM et d'actifs communs se trouvent au même niveau que pour MDB r1.5. Pour plus d'informations, consultez la section Préparation du travail avec la MDB Microsoft SQL (page 135) ou Préparation du travail avec la MDB Oracle (page 139).

Pour des informations générales sur la MDB, notamment son déploiement et son administration, reportez-vous au document *Présentation de la MDB*, disponible dans la documentation en ligne de CA Client Automation (Bibliothèque).

Dans l'architecture à plusieurs niveaux, les instances de la base de données de gestion (MDB) peuvent être implémentées au niveau du gestionnaire d'entreprise et de domaine. Ces deux niveaux prennent en charge les MDB Microsoft SQL Server et Oracle. Vous pouvez également implémenter les MDB sur différents fournisseurs de base de données sur les niveaux individuels. Par exemple, vous sélectionnez SQL Server pour le gestionnaire de domaine et Oracle pour le gestionnaire d'entreprise.

Dans les configurations mixtes, par exemple un gestionnaire de domaine avec une MDB basée sur SQL Server et un gestionnaire d'entreprise avec une MDB basée sur Oracle, vous avez besoin des clients de bases de données appropriés sur les gestionnaires ; dans cet exemple, vous avez besoin du client Oracle sur le gestionnaire de domaine et du client SQL sur le gestionnaire d'entreprise.

Actuellement, une MDB basée sur Oracle est uniquement prise en charge en tant que base de données distante sur un système d'exploitation Sun Solaris. Pour plus d'informations sur les versions de la base de données et les environnements d'exploitation actuellement pris en charge, consultez les *notes de parution CA Client Automation*, disponibles dans la documentation de CA Client Automation (Bibliothèque).

Les scénarios de base de données pris en charge sont les suivants :

MDB SQL Server locale

Gestionnaire de domaine ou d'entreprise DSM sous Windows avec la MDB située sur le même ordinateur et basée sur SQL Server.

MDB SQL Server distante

Gestionnaire de domaine ou d'entreprise DSM sous Windows avec la MDB située sur un serveur distant et un ordinateur exécutant Windows, et basée sur SQL Server.

MDB Oracle distante

Gestionnaire de domaine ou d'entreprise DSM sous Windows avec la MDB située sur un serveur distant et un ordinateur exécutant Solaris, et basée sur Oracle.

Toutes les MDB au sein de la structure d'entreprise et de domaine présentent le même schéma. Les bases de données de domaine contiennent les informations sur la manière de se connecter au gestionnaire d'entreprise. La base de données d'entreprise contient les informations sur la manière de se connecter à l'ensemble des domaines qui y sont reliés, ainsi que sur les gestionnaires disponibles et leur emplacement.

Client Automation propose une fonctionnalité qui vous permet de synchroniser les données collectées sur une MDB Microsoft SQL Server sur un gestionnaire de domaines ou d'entreprise avec les données d'une MDB SQL Server distante ou une MDB Oracle. Cette fonctionnalité de synchronisation de base de données prend en charge, par exemple, les installations existantes des produits CA Technologies Service Desk Manager et Asset Portfolio Management qui utilisent une MDB SQL Server ou Oracle. Pour plus d'informations sur la fonctionnalité de synchronisation, consultez Synchronisation des données à partir d'une MDB vers une MDB cible séparée. (page 33)

Remarque : Pour totalement prendre en charge le produit d'intégration Unicenter Asset Portfolio Management, vous devez installer le patch RO02252. Pour des instructions d'installation, consultez le fichier Readme Unicenter Asset Portfolio Management, RO02252. Pour plus d'informations concernant Unicenter Asset Portfolio Management et CA Service Desk Manager, reportez-vous aux documentations correspondantes.

Installation de la base de données de gestion (MDB, Management Database)

La base de données de gestion (MDB) peut être installée localement sur le gestionnaire ou sous forme de MDB distante sur un ordinateur séparé, en fonction des exigences fixées en matière de modularité et de performances. L'installation de la MDB sur Windows et Solaris est prise en charge par les kits d'installation DSM.

Pour plus de détails sur l'installation de la MDB, consultez la section Base de données de gestion (MDB) (page 126) du chapitre "Installation de Client Automation".

Administration de la MDB

L'administration des bases de données est capitale pour le bon fonctionnement et les performances de la base de données de gestion (MDB). Pour vous assister dans cette tâche, CA Technologies propose des scripts de maintenance de la MDB sur le support d'installation de CA Client Automation (DVD).

Pour plus de détails sur la maintenance de la MDB, consultez la section Base de données de gestion (MDB) (page 126) du chapitre "Installation de Client Automation". Pour plus d'informations sur les exigences spécifiques d'administration de la MDB, en termes de configuration et de maintenance, reportez-vous au document *Présentation de la MDB*, dans la documentation pour CA Client Automation (Bibliothèque).

Concept Moteur

Le moteur est un processus qui fournit des services de communications entre les serveurs de modularité, le gestionnaire de domaine et la base de données de gestion.

Les fonctions d'un moteur sont les suivantes :

- La collecte de l'inventaire des ordinateurs depuis un serveur de modularité
- L'écriture de données de configuration sur un serveur de modularité
- La copie de données entre les bases de données de domaine et Enterprise (réplication)
- L'évaluation dynamique des groupes de requêtes
- L'exécution d'actions en rapport avec l'évaluation des groupes de requêtes
- L'exécution de rapports planifiées
- La communication de l'état d'un job d'inventaire

Aspects administratifs du moteur

Vous pouvez consulter l'état des tâches du moteur via l'explorateur DSM. Cet explorateur permet d'ajouter, de modifier ou de supprimer des tâches de moteur.

Chaque instance d'un gestionnaire de domaine et d'entreprise comprend un moteur par défaut appelé Moteur système.

Il est possible d'installer des moteurs supplémentaires pour alléger la charge de travail de ce moteur par défaut.

Chaque fois qu'un nouveau serveur de modularité est déployé, une tâche de collecte de moteur est automatiquement créée et programmée pour le moteur système par défaut. Il est possible de charger un autre moteur de cette tâche pendant le processus d'installation de serveur de modularité.

Chaque fois qu'un gestionnaire de domaine est lié à un gestionnaire d'entreprise, une tâche de réplication de moteur est automatiquement créée et liée au Moteur système par défaut.

Collecte d'informations

La tâche principale d'un moteur consiste à collecter des informations sur les actifs à partir des serveurs de modularité.

Lorsqu'un agent DSM se connecte pour la première fois à un serveur de modularité, il soumet une création de requête et stocke les informations initiales de l'inventaire et du système.

Lorsqu'un moteur se connecte à un serveur de modularité, il effectue les tâches suivantes :

1. Contrôler l'intégrité du serveur de modularité.
2. Déterminer si des agents sont connectés pour la première fois à ce serveur.
3. Si les actifs sont nouveaux pour l'ensemble du système, il les crée dans la base de données.
4. Traiter toutes les informations d'inventaire fournies par les agents existants.

Les informations collectées peuvent se présenter sous les formes suivantes :

- Inventaire (informations matérielle ou de modèle)
- Inventaire logiciel (heuristique ou basé sur une signature)
- Fichiers de configuration (fichiers autoexec.bat ou n'importe quel fichier .INI configuré pour être sauvegardé)
- Etat du job
- Etat du module
- Date et heure de la dernière exécution de l'agent
- Données de surveillance de l'utilisation des logiciels
- Informations sur les relations (entre ordinateurs, utilisateurs et unités)

Réplication de données entre Enterprise et domaine

Une autre tâche du moteur consiste à répliquer des données entre les bases de données Entreprise et Domaine. La réplication à partir de la base de données de gestion sur le gestionnaire de domaine vers la base de données de gestion sur le gestionnaire de domaine est exécutée à l'aide d'un job de réplication exécuté via le processus du moteur du gestionnaire de domaine.

Lorsque la réplication commence, le moteur détermine quelles informations doivent être transmises à partir du domaine vers le gestionnaire d'entreprise et lesquelles doivent être transmises à partir de l'entreprise vers le gestionnaire de domaine.

Généralement, les informations spécifiques à l'hôte, telles que les attributs d'inventaire, sont transmises au niveau supérieur, tandis que les informations de configuration, telles que les groupes d'actifs, sont transmises au niveau inférieur.

Un moteur par défaut est installé avec chaque gestionnaire de domaines. Lorsque le gestionnaire de domaines est relié à un gestionnaire d'entreprise, ce moteur est configuré pour effectuer les tâches de réplication entre le domaine et Enterprise.

Objets de base de données dupliqués

Le tableau ci-dessous répertorie les objets de base de données qui sont répliqués à partir du gestionnaire d'entreprise vers le gestionnaire de domaine (descendant) et à partir du gestionnaire de domaine vers le gestionnaire d'entreprise (ascendant).

Object	Direction de la réplication
Ordinateurs détectés	ascendant
Utilisateurs détectés	ascendant
Utilisateurs d'ordinateurs détectés (relations entre ordinateurs et utilisateurs)	ascendant

Object	**Direction de la réplication**
Ordinateurs du carnet d'adresses Remote Control	descendant
Définitions d'actifs externes	descendant
Actifs externes	ascendant
Inventaire général des ordinateurs	ascendant
Composants supplémentaires de l'inventaire **Remarque :** Par défaut, ces objets ne sont pas dupliqués. Pour activer/désactiver leur réplication, cliquez avec le bouton droit de la souris sur le noeud Inventaire/Supplémentaire/<*nom-du-module*> de l'agent et sélectionnez l'option Répliquer l'analyse heuristique vers la BdD de l'entreprise. La configuration modifiée est appliquée à tous les ordinateurs du groupe.	ascendant
Inventaire des actifs externes	ascendant
Définitions des requêtes	descendant
Définitions de groupe	descendant
Adhésion au groupe	descendant
Définitions de logiciels personnalisés	descendant
Fabricant personnalisé	descendant
Propriétés du gestionnaire d'entreprise	descendant
Propriétés du gestionnaire de domaine	ascendant
Inventaire logiciel des ordinateurs (basé sur une analyse des signatures)	ascendant
Inventaire logiciel découvert par l'analyse heuristique **Remarque :** Par défaut, cet objet n'est pas dupliqué. Pour activer/désactiver sa réplication, cliquez avec le bouton droit de la souris sur le noeud Logiciel/Détecté de l'agent et sélectionnez l'option Répliquer l'analyse heuristique vers la BdD de l'entreprise. La configuration modifiée est appliquée à tous les ordinateurs du groupe.	ascendant
Jobs Asset Management	descendant
Etat du job Asset Management	ascendant
Modules Asset Management	descendant
Etat des modules Asset Management	ascendant
Définitions de fichier de configuration Asset Management	descendant
Fichiers de configuration Asset Management **Remarque :** Ces fichiers sont dupliqués uniquement vers le gestionnaire d'entreprise si la demande de collecte de ces informations a été définie sur le gestionnaire d'entreprise. Si la demande a été définie sur le gestionnaire de domaines, les données ne sont pas dupliquées de manière ascendante.	ascendant

Object	Direction de la réplication
Définition des modèles Asset Management	descendant
Définitions de stratégies Asset Management	descendant
Alertes de surveillance de l'intégrité	ascendant

Synchronisation des données à partir d'une MDB vers une MDB cible séparée

Dans certaines implémentations, les clients souhaitent que certains produits CA Technologies, tels que Service Desk et Asset Portfolio Management, utilisent des bases de données de gestion (MDB) séparées ou différentes de la base de données utilisée par le gestionnaire DSM.

Cependant, dans de nombreux aspects de leurs tâches Asset Management, ces produits CA Technologies s'appuient sur des données Client Automation.

Par conséquent, Client Automation offre des fonctions de gestion qui prennent en charge et synchronisent les données découvertes par Client Automation sur une MDB séparée pouvant être basée sur Microsoft SQL Server (SQL Bridge) ou Oracle (Oracle Bridge). Ces fonctionnalités synchronisent les données d'actifs et d'inventaire Client Automation collectées dans la MDB SQL Server sur le gestionnaire de domaine ou d'entreprise exécutant Windows avec les données correspondantes dans la MDB cible SQL Server ou Oracle.

La synchronisation est lancée par une tâche de moteur qui s'exécute à l'heure planifiée. C'est vous qui créez cette tâche du moteur et définissez la planification de la tâche à l'aide de l'assistant de création des tâches du moteur via l'interface graphique de l'explorateur DSM. Vous pouvez utiliser un autre moteur sur un ordinateur distant pour effectuer la synchronisation.

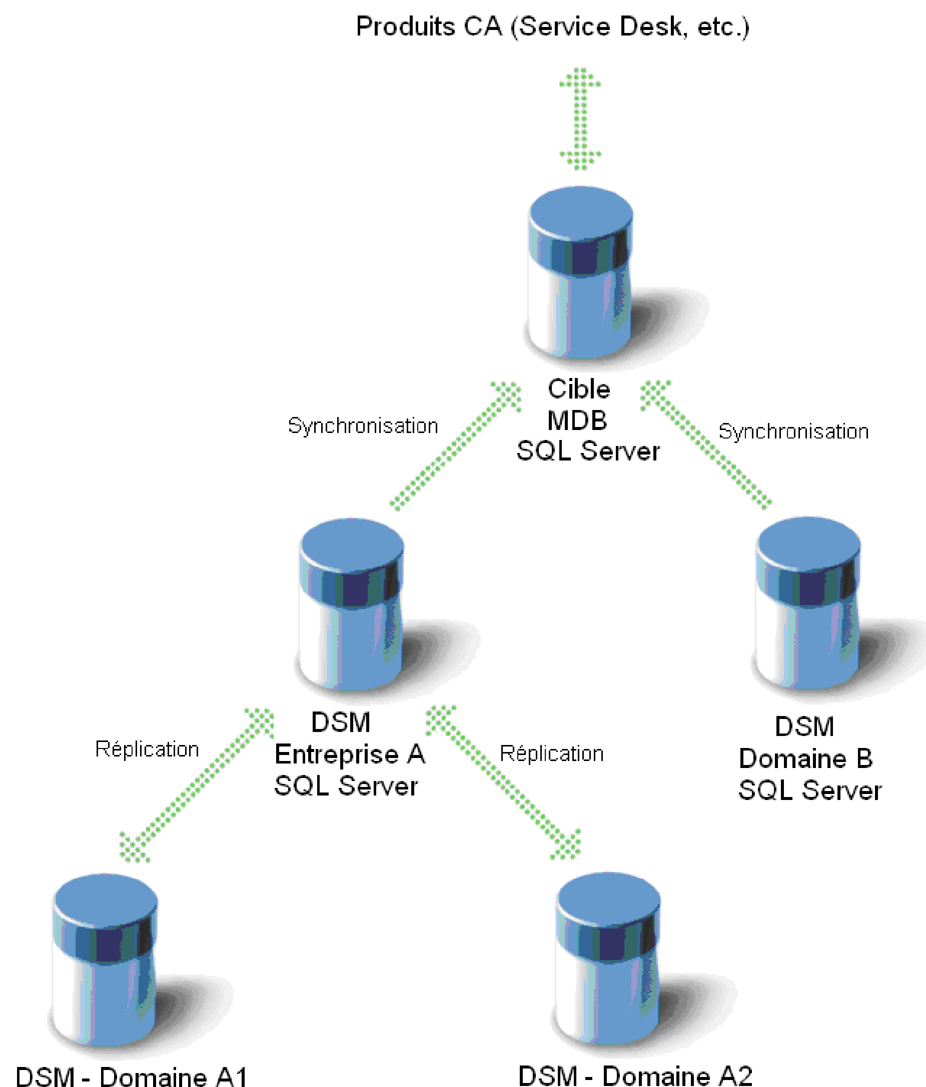
Pour plus d'informations, consultez la section Base de données de gestion (MDB) (page 126) du chapitre "Installation de Client Automation".

Architecture du mécanisme de synchronisation

Le mécanisme de synchronisation est similaire au mécanisme de réplication utilisé entre le gestionnaire de domaines DSM et le gestionnaire d'entreprise.

La synchronisation est réalisée dans un sens, des gestionnaires vers la MDB cible. Cela signifie que si les données synchronisées sont modifiées sur la MDB cible par un autre processus, elles seront écrasées la prochaine fois que la méthode de synchronisation déplace cet ensemble particulier de données de la MDB des gestionnaires à la MDB cible.

L'illustration suivante présente un scénario spécial où la synchronisation est réalisée d'un gestionnaire d'entreprise à un gestionnaire de domaine, les deux hébergeant leurs MDB sur Microsoft SQL Server, à une MDB cible SQL Server.



Dans un autre scénario, la MDB cible peut être exécutée sur Oracle. Il est également possible de synchroniser d'une MDB SQL Server sur un gestionnaire d'entreprise ou de domaine vers deux différentes MDB cibles.

Scénarios de base de données pris en charge

Pour obtenir des informations sur la prise en charge des fonctionnalités de synchronisation SQL Bridge et Oracle Bridge, consultez la matrice de compatibilité.

Scénarios de base de données pris en charge pour SQL Bridge et Oracle Bridge

Si vous avez installé CA Service Desk Manager ou CA IT Asset Manager sur une MDB SQL Bridge ou Oracle Bridge, vous pouvez synchroniser les informations remplies par les clients hébergés dans la base de données Client Automation.

- Pour consulter des scénarios de bases de données prises en charge par les fonctionnalités de synchronisation SQL Bridge et Oracle Bridge, reportez-vous à la matrice de compatibilité.

Prise en charge des produits CA Technologies

Pour obtenir des informations sur les fonctionnalités de synchronisation SQL Bridge et Oracle Bridge pour les MDB basées sur SQL Server et sur Oracle qui prennent en charge les produits CA Technologies, CA Service Desk Manager et Unicenter Asset Portfolio Management, consultez la matrice de compatibilité.

- **SQL Bridge :**

  Pour profiter pleinement de SQL Bridge, il faut installer le correctif de test T5D6008 pour Windows sur les ordinateurs où CA Service Desk Manager r11.2 et Unicenter Asset Portfolio Management r11.3 sont installés. Le correctif de test est disponible sur le support CA en ligne. Téléchargez le correctif de test et suivez les instructions détaillées d'installation fournies dans le fichier lisez-moi qui accompagne le correctif de test.

- **Oracle Bridge :**

  Pour profiter pleinement d'Oracle Bridge, il faut ajouter un nouveau paramètre, dsm_oracle_ddl, au fichier AMS.properties pour CA Service Desk Manager afin d'activer Oracle Bridge :

  ```
  dsm_oracle_ddl=1
  ```

Pour plus d'informations sur l'installation de SQL Bridge et Oracle Bridge dans votre environnement d'application, consultez les sections Installation de SQL Bridge (page 229)et Installation d'Oracle Bridge (page 230).

Serveur de modularité.

Dans Client Automation, l'interface entre les agents et leur gestionnaire de domaines est fournie par un serveur de modularité.

Le premier rôle du serveur de modularité consiste à répartir entre plusieurs hôtes la charge de travail due à la gestion d'agents indépendants. Au lieu que tous les agents communiquent directement avec un seul gestionnaire, la charge peut être partagée sur plusieurs serveurs de modularité. Par exemple, les packages logiciels sont transférés sur un serveur de modularité avant leur téléchargement vers les systèmes finals, et l'inventaire peut être stocké sur le serveur de modularité avant son téléchargement sur le gestionnaire.

Avec les applications virtualisées, le serveur de modularité fonctionne aussi en tant que serveur de diffusion en continu pour les packages d'application virtualisée qui sont diffusés vers des ordinateurs cibles exécutant des systèmes d'exploitation Windows.

Un serveur de modularité se compose de plusieurs processus système qui s'exécutent en arrière-plan sans interface utilisateur visible.

Sous-composants du serveur de modularité standard

L'installation d'un serveur de modularité standard comporte les sous-composants suivants :

- Cadre d'applications (avec fonction d'enregistrement)
- Fonction de serveur commun

  Le serveur de modularité peut recevoir des requêtes d'enregistrement et des informations d'inventaire standard de la part des agents, procéder aux enregistrements avec des gestionnaires et recevoir du gestionnaire, ou lui transmettre, différentes notifications et informations de gestion.

- Base de données de stockage des fichiers

  La base de données de stockage des fichiers est un référentiel local utilisé par le serveur de modularité pour stocker les informations requises pour servir les agents. Dans une installation minimale de serveur de modularité, la base de données de fichiers se compose d'un dictionnaire des agents enregistrés et de l'inventaire standard signalé par ces derniers.

Tâches de serveur de modularité standard

Un installation de serveur de modularité standard peut effectuer les tâches suivantes :

- Fournit un mécanisme d'enregistrement pour la connexion des agents.
- Reçoit l'inventaire standard transmis par les agents.
- Enregistre le serveur de modularité auprès d'un gestionnaire.
- Reçoit la configuration du serveur de modularité transmise par le gestionnaire.
- Fait suivre l'enregistrement des agents et les informations d'inventaire standard requises par le gestionnaire.
- Fait suivre les configurations d'agent transmises depuis le gestionnaire.

En outre, d'autres tâche spécifiques au produit peuvent être activées pour les fonctions Asset Management, Remote Control et Software Delivery (y compris la gestion de l'installation du système d'exploitation).

Un agent Software Delivery (SD) est installé avec chaque serveur de modularité pour permettre aux fonctions SD du serveur de modularité de fonctionner correctement. Afin d'éviter tout dysfonctionnement du serveur de modularité, ne tentez en aucun cas de supprimer l'agent SD du serveur de modularité.

L'agent du serveur de modularité doit également s'inscrire auprès de ce serveur de modularité et d'aucun autre. Pour vérifier cela, vous pouvez exécuter caf setserveraddress sur le serveur de modularité avec le résultat de localhost, ou une adresse équivalente indiquant l'hôte local. Si l'adresse renvoyée indique un serveur de modularité différent, vous pouvez rectifier cela en exécutant la commande caf setserveraddress localhost sur le serveur de modularité en question.

Déploiement du serveur de modularité et de l'application virtualisée

L'assistant d'enregistrement de packages d'application virtualisée (que vous utilisez pour importer des images d'application virtualisée et pour créer des packages dans la bibliothèque de packages logiciels) crée les packages logiciels suivants pour chaque image d'application virtualisée :

- Stockage intermédiaire : ce package permet d'accéder à l'application virtualisée dans les deux modes de livraison de packages (autonome et de diffusion en continu). et contient l'image d'application virtualisée.
- Autonome : ce package est utilisé pour installer et exécuter l'application virtualisée localement sur l'ordinateur cible.
- Diffusion en continu : ce package est utilisé pour diffuser en aval l'application virtualisée à partir d'un serveur de diffusion en continu et s'exécute sur l'ordinateur local.

Le package de stockage intermédiaire d'application virtualisée se déploie vers le serveur de modularité. Le serveur de modularité fonctionne également en tant que serveur de diffusion en continu pour les applications virtualisées. Par conséquent, les packages de stockage intermédiaire sont déployés vers le serveur de modularité pour diffuser en continu l'application virtualisée vers les ordinateurs cibles.

Le serveur de diffusion en continu de Microsoft App-V utilise deux protocoles pour des communications de diffusion en continu : RTSP (non sécurisé) et RTSPS (sécurisé). Le protocole par défaut pour le serveur de diffusion en continu de Microsoft App-V est RTSP et le port, 554. Pour utiliser le protocole sécurisé RTSPS avec le port 322, configurez le serveur de diffusion en continu. Pour plus d'informations sur la configuration du serveur de diffusion en continu de Microsoft App-V, reportez-vous à la documentation de produit Microsoft.

Le déploiement des packages autonomes et de diffusion en continu s'effectue du gestionnaire de domaines aux ordinateurs cibles. Vous pouvez également stocker les packages de façon intermédiaire sur le serveur de modularité avant le déploiement vers les ordinateurs cibles. Vous pouvez utiliser les méthodes standard de déploiement Software Delivery pour déployer des packages d'application virtualisée vers des ordinateurs cibles.

Remarque : Pour plus d'informations sur le packaging et le déploiement d'applications virtualisées, consultez le *Manuel d'administration de Software Delivery*.

Aspects relatifs à l'installation du serveur de démarrage de gestion de l'installation du système d'exploitation

Le serveur amorçable de gestion d'installation de système d'exploitation (OSIM, OS Installation Management) est installé comme composant d'un serveur de modularité. L'installation du serveur de démarrage fournit automatiquement un serveur TFTP (avec des droits d'accès restreints) et un serveur PXE.

Si vous ne voulez pas utiliser cette fonction, vous pouvez désactiver le service de serveur de démarrage au cours de l'installation du serveur de modularité ou en exécutant ultérieurement les commandes CAF suivantes :

```
caf stop sdmpcserver
```

```
caf disable sdmpcserver
```

Si vous voulez réactiver le service de serveur de démarrage ultérieurement, lancez ces commandes CAF :

```
caf enable sdmpcserver
```

```
caf start sdmpcserver
```

Agent

Des agents existent sur tous les systèmes finaux gérés se trouvant sur tous les environnements de fonctionnement pris en charge, où chacun des agents effectue des tâches individuelles.

Lorsqu'un agent est enregistré dans le gestionnaire CA ITCM, l'UUID de l'hôte est l'attribut principal utilisé pour mettre en correspondance l'ordinateur à un enregistrement d'ordinateur existant dans la MDB. Si l'UUID de l'hôte ne renvoie aucune correspondance, le nom d'hôte et les adresses MAC sont utilisés pour la mise en correspondance de l'ordinateur.

Si une correspondance au nom d'hôte et aux adresses MAC est renvoyée, cela signifie que l'UUID d'hôte de l'ordinateur a été modifié. Par exemple, la réinstallation du système d'exploitation entraîne un changement de l'UUID d'hôte de l'ordinateur respectif. L'enregistrement d'ordinateur est alors mis à jour avec le nouvel UUID d'hôte et un conteneur de job de livraison de logiciels Réinstaller après un arrêt brutal est créé.

Si aucune correspondance n'est renvoyée pour le nom d'hôte et les adresses MAC, un nouvel ordinateur est créé et aucun conteneur de jobs Réinstaller après un arrêt brutal n'est créé.

Dans certains cas, un ordinateur dupliqué peut être créé au lieu d'effectuer la mise en correspondance d'un enregistrement existant. Pour corriger ce problème, l'algorithme de mise en correspondance du nom d'hôte et des adresses MAC a été amélioré. Auparavant, seule l'adresse MAC principale était utilisée pour la mise en correspondance des adresses MAC existantes. Désormais, l'ensemble des adresses MAC standard de l'ordinateur est utilisé. Les adresses MAC standard excluent les adresses MAC transitoires (par exemple, celles d'un réseau privé virtuel), qui pourraient renvoyer des correspondances incorrectes.

Le tableau ci-dessous récapitule les cas où un nouvel ordinateur est créé et mis en correspondance avec un ordinateur existant, lorsque l'un des UUID d'hôte, des noms d'hôte ou des adresses MAC sont modifiés.

Remarque : Le trait d'union (-) utilisé dans le tableau indique que le système ignore la recherche de modifications.

Modification de l'UUID d'hôte	Modification du nom d'hôte	Modification de toutes les adresses MAC standard	Modification de l'adresse MAC principale	Création d'un actif	RAC
N	-	-	-	N	N
Y	N	N	-	N	Y
Y	N	-	N	N	Y
Y	N	Y	Y	Y	N
Y	Y	-	-	Y	N

Remarque : Dans un environnement comprenant des machines virtuelles (par exemple XenServer, Hyper-V ou ESX), l'administrateur doit s'assurer que chaque machine virtuelle dispose d'une adresse MAC unique dans l'espace de domaine.

Remarque : Lorsqu'un ordinateur est préenregistré, l'administrateur doit s'assurer qu'une adresse MAC standard a été entrée.

Le concept des packages d'agent

Le concept des packages d'agent (agents DSM) dans Client Automation distingue les fonctionnalités réelles de l'agent des ressources linguistiques individuelles. Ce concept offre les avantages suivants en termes de déploiement et d'installation de l'agent :

- **Packages linguistiques des agents**

  Le concept des packages d'agent vous permet d'installer séparément les packages linguistiques. Un package linguistique contient toutes les ressources linguistiques dans une seule langue requise par une installation d'agent.

- **Capacité à créer un seul package d'installation contenant uniquement les composants obligatoires**

  Le script dsmPush permet de créer des packages d'installation personnalisés, par exemple un package unique comprenant des fonctions Asset Management et Software Delivery avec six packages linguistiques.

Le format des packages d'agent associe les fonctionnalités des agents avec ou sans packages linguistiques. Si aucun package linguistique n'est spécifié, ENU (anglais (Etats-Unis)) est utilisé par défaut. Les ressources ENU sont toujours incluses dans la fonctionnalité d'agent et ne font, par conséquent, pas l'objet d'un package linguistique distinct. Vous pouvez toutefois déployer un package linguistique autonome sur un agent.

Remarque : Pour plus d'informations sur les packages linguistiques, consultez la section Modification de la langue du produit après l'installation dans le chapitre "Installation de Client Automation".

L'agent DSM peut posséder les modules d'extension suivants :

- Agent DSM CA + module d'extension Software Delivery (agent SD)
- Agent DSM CA + module d'extension Remote Control (agent RC)
- Agent DSM CA + module d'extension Asset Management (agent AM)
- Agent DSM CA + module d'extension d'inventaire de base (agent BHI)
- Catalogue Software Delivery (catalogue SD)
- Visionneuse Remote Control (visionneuse RC)
- Tous les composants côté agent, par exemple le service de transport de données (DTS)

Configuration d'agent

Les agents sont gérés de façon centralisée et configurés par leur gestionnaire de domaine. Ces tâches sont effectuées à l'aide de l'explorateur DSM.

Visionneuse Remote Control

La visionneuse Remote Control (visionneuse RC) constitue l'interface utilisateur assurant l'accès aux services Remote Control. Lorsqu'elle est installée, vous pouvez accéder à la visionneuse RC depuis l'arborescence de l'explorateur DSM ou en utilisant la ligne de commande.

La fonction Remote Control prend en charge un navigateur client Win32 ou Web. Le navigateur client nécessite l'installation de Microsoft Internet Explorer 6.0.

Parmi les fonctions propres à la visionneuse RC, notons :

Remote Control

Vous permet d'agir comme si vous étiez assis devant l'ordinateur que vous contrôlez.

Transfert de fichiers

Transfère des fichiers entre la visionneuse et les ordinateurs hôte.

Discussion instantanée

Permet de discuter avec un utilisateur pendant une session de contrôle à distance.

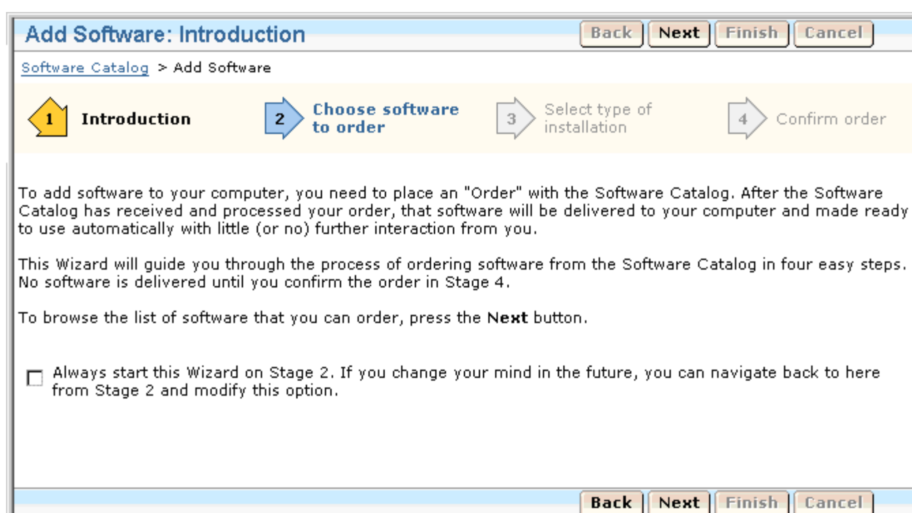
Enregistrement de la session

Démarre et arrête l'enregistrement de la session de contrôle à distance.

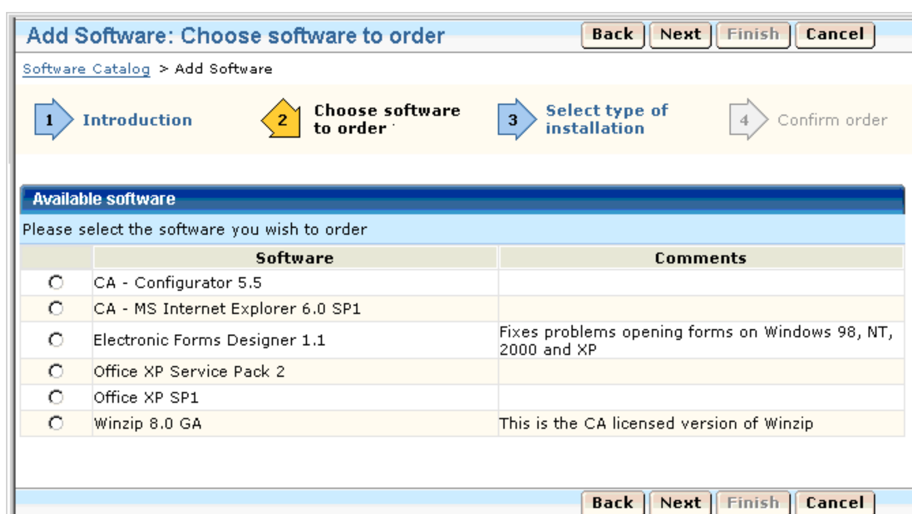
Catalogue de logiciels

Le catalogue de logiciels (également appelé catalogue Software Delivery ou catalogue SD) est un module d'extension d'agent qui vous offre un "self-service". Grâce à l'interface basée sur l'assistant du catalogue de logiciels, vous pouvez installer ou supprimer des logiciels de votre ordinateur à partir d'une bibliothèque fournie par l'administrateur.

La capture d'écran suivante montre la page d'"Introduction" de l'Assistant Ajout de logiciels :



La capture d'écran suivante montre un exemple de page "Sélection des logiciels à commander" de l'assistant Ajout de logiciels :



Agent distant AM

Client Automation prend en charge la virtualisation de plates-formes, y compris les environnements UNIX virtualisés suivants :

- nPartitions et partitions virtuelles HP
- Ordinateurs Integrity Virtual Machines
- Partitions logiques IBM
- Domaines de systèmes dynamiques Sun
- Domaines de système dynamique Sun sur des serveurs Sun SPARC Enterprise M-series
- Machines virtuelles exécutées sous VMware ESXi
- Machines virtuelles exécutées sous Citrix XenServer

L'agent distant AM remplace l'agent du serveur UNIX partitionné r12, mais sa fonctionnalité a été complètement intégrée à l'agent distant AM. Cet agent est configuré exclusivement dans l'explorateur DSM pour collecter les informations des hôtes virtuels.

Remarque : Pour des informations détaillées sur l'agent distant AM, consultez le *Manuel d'administration d'Asset Management*. Pour obtenir la liste la plus récente des plates-formes prises en charge, consultez la matrice de compatibilité.

Console Web

La console Web est une interface utilisateur basée sur un navigateur de CA Client Automation qui peut être installée sur les environnements d'exploitation Windows et Linux.

La console Web peut être installée sur le même ordinateur que le gestionnaire ou sur un autre ordinateur (console Web distante).

Accès à la console Web

Pour vous connecter à la console Web, il vous suffit d'ouvrir un navigateur et d'entrer l'URL suivante dans la barre d'adresse :

`http://MonGestionnaire/wac`

MonGestionnaire est le nom DNS, le nom de l'hôte ou l'adresse IP de l'ordinateur sur lequel vous avez installé la console Web. La console Web vous connecte automatiquement avec les informations d'identification que vous avez fournies pour vous connecter à l'ordinateur. La page de connexion à la console Web affiche une liste déroulante qui vous permet d'utiliser un gestionnaire différent.

Possibilités de la console Web

La console Web vous permet d'accéder aux objets DSM via un volet de recherche à la fois simple et puissant. Après avoir localisé un objet, l'utilisateur peut utiliser les onglets, portlets, sections de pages et liens de navigation, qui fournissent une interface étendue de type navigateur.

La console Web présente à l'utilisateur une vue complète des informations de DSM. En fonction des produits et des composants installés, elle peut inclure les éléments suivants :

- Ordinateurs
- Groupes
- utilisateurs
- Packages logiciels
- Définitions de logiciels
- Jobs
- Politiques
- Requêtes
- Alertes

La console Web permet aussi à l'utilisateur de mener les activités suivantes (si les produits et composants appropriés ont été installés) :

- Création et suppression d'ordinateurs
- Création, modification et suppression des groupes
- Jobs d'installation de système d'exploitation
- Installation des logiciels
- Désinstallation des logiciels
- Configuration de job d'installation de logiciel
- Surveillance et suivi des alertes de surveillance d'intégrité

La console Web peut être démarrée dans le cadre d'un job ou d'une stratégie via une URL depuis n'importe quelle autre application disposant d'un accès à l'UUID d'un objet approprié.

La console Web est également capable de lancer l'application CA Service Desk Manager dans le cadre d'un ticket (problème) qui a été soulevé suite à une violation de stratégie ou à un échec de job logiciel.

Navigateurs Web et serveurs Web pris en charge

Pour des informations sur la prise en charge des navigateurs et des serveurs Web, consultez la matrice de compatibilité.

Générateur de rapports DSM

Le générateur de rapports DSM est un outil de requête utilisé pour extraire des informations de la base de données.

La génération des rapports peut être ad hoc ou planifiée. Le générateur de rapports DSM optimise la valeur des données Client Automation en les organisant, les filtrant et les présentant. Le générateur de rapports DSM offre également la possibilité d'exporter des données dans des fichiers CSV (*.csv) ou HTML (*.html). Vous pouvez ensuite importer ces fichiers dans des tableurs, des outils de budgétisation, etc.

L'apparence du générateur de rapports DSM reste similaire à celle de l'explorateur DSM. Les options de glisser-déplacer pour l'impression d'unités et de groupes Client Automation ainsi que pour la création de rapports sur la base de requêtes renforcent la perception du générateur de rapports DSM comme une extension de l'explorateur DSM.

Remarque : Lorsque vous lancez le générateur de rapports DSM pour la première fois après l'installation, prévoyez assez de temps pour importer tous les modèles de rapport dans la base de données. Toutefois, si une erreur se produit pendant l'importation des modèles de rapport, vous pouvez corriger le problème en ouvrant l'éditeur de registre et en supprimant la sous-clé dans HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Unicenter ITRM\Reporter\Library. Après avoir supprimé la sous-clé, relancez le générateur de rapports DSM.

Cadre d'applications communes

Chacun des composants DSM utilise le cadre d'applications communes (CAF, Common Application Framework). CAF est un contrôleur de service inter-plate-forme qui offre un point de contrôle unique pour tous les composants DSM.

CAF fournit de manière dynamique les services DSM en fonction des besoins, via un modèle de module d'extension extensible. Chaque module d'extension CAF est un programme qui fournit les fonctionnalités d'agent, de serveur de modularité ou de gestionnaire. Un module d'extension CAF peut également être une extension de CAF qui offre certains services communs, par exemple l'enregistrement auprès de serveurs de modularité ou la détection d'événements système.

Normalement, CAF démarre automatiquement tous les modules d'extension lors du démarrage. CAF peut également démarrer et arrêter les modules d'extension à la demande à partir de la ligne de commande, à des heures particulières et à des intervalles réguliers, via le planificateur. Pour une description du mode de spécification des jobs programmés qui s'exécutent dans CAF, reportez-vous à l'annexe Jobs planifiés CAF (page 609).

CAF peut également interroger des module d'extensions afin d'obtenir des informations d'état, et acheminer des messages provenant d'autres module d'extensions.

Important : Sous Windows, CAF est installé par défaut pour ouvrir une session sous le compte Système local. Si, pour des raisons de sécurité, vous devez changer cette propriété de connexion réseau, vous devez le faire après l'installation via la console Gestion de l'ordinateur, Services, à partir du Panneau de configuration Windows. Cependant, le passage à un compte doté de privilèges réduits peut entraîner un comportement DSM inattendu ou des fonctionnalités réduites de CA Client Automation.

Interface utilisateur de cadre d'applications

Il n'est normalement pas nécessaire d'avoir une interaction avec le cadre d'applications communes (CAF), car il s'exécute en tant que service en arrière-plan. Cependant, le CAF comprend une interface de ligne de commande (commande caf) qui permet aux administrateurs d'accéder, localement ou à distance, à la fonctionnalité CAF, comme dans les exemples suivants :

- Requête de l'état actuel de tous les modules d'extension CAF
- Démarrer et arrêter CAF, ainsi que tous les modules d'extension et processus associés
- Démarrer, arrêter et interroger l'état d'un module d'extension individuel
- Activer et désactiver des modules d'extension

L'interface de ligne de commande CAF, dans la plupart des cas, ne fait qu'envoyer un message à CAF, lui demandant d'exécuter la commande. Les exceptions sont les commandes permettant de démarrer et d'arrêter le service ou démon CAF proprement dit, ainsi que quelques commandes de configuration.

Remarque : Sous Windows Vista, la plupart des commandes caf nécessitent des droits d'administrateur complets. Si vous êtes membre du groupe d'administrateurs, mais que vous êtes connecté en tant qu'utilisateur quelconque non administrateur, une fenêtre de ligne de commande s'exécutera normalement avec les droits de l'utilisateur. Pour exécuter des commandes caf, vous devez exécuter la fenêtre de ligne de commande en cliquant sur l'icône correspondante et en sélectionnant Exécuter en tant qu'administrateur.

Barre d'état système

La barre d'état système est un outil permettant à l'utilisateur d'accéder aux services système, tels que les services CAF (Common Application Framework, cadre d'applications communes).

La barre d'état système apparaît sous la forme d'une icône dans la barre des tâches sur le Bureau de tous les systèmes d'exploitation, sauf sous UNIX. Lorsque vous cliquez sur l'icône avec le bouton droit de la souris, vous pouvez sélectionner l'un des services disponibles dans le menu contextuel. Si nécessaire, la fonction de la barre d'état système peut requérir une autre intervention de l'utilisateur avant de démarrer le service.

Les services disponibles via la barre d'état système et la visibilité des icônes de la barre d'état système dans la barre des tâches (affichées ou masquées) varient en fonction de la stratégie de configuration.

Lors de l'exécution de Client Automation, vous pouvez contrôler la barre d'état système et ses icônes depuis la ligne de commande à l'aide des commandes suivantes :

cfSysTray

Permet de démarrer la barre d'état système si son état est défini sur Afficher dans la stratégie de configuration. L'icône apparaît dans la barre des tâches.

cfSysTray show

Permet de démarrer la barre d'état système (si ce n'est pas déjà le cas) et de définir son état sur Afficher dans la stratégie de configuration. L'icône apparaît dans la barre des tâches.

cfSysTray stop

Arrête la barre d'état système. L'icône Barre d'état système n'apparaît plus dans la barre des tâches.

cfSysTray hide

Permet d'arrêter la barre d'état système et de définir son état sur Masquer dans la stratégie de configuration. L'icône Barre d'état système n'apparaît plus dans la barre des tâches.

Sous Linux, la barre d'état système Client Automation requiert l'installation de GIMP Toolkit GTK+ 1.2 (version minimum). Le GTK n'est pas équipé de Client Automation ; vous devez télécharger la version requise à l'adresse suivante www.gtk.org.

Journalisation

La bibliothèque de composants communs (CCL) prend en charge le suivi complet et comporte un gestionnaire de défaillance pour vous aider à diagnostiquer les erreurs irrécupérables. Ces services sont disponibles pour et exploités par la plupart des modules d'extension.

Les services CAF consignent leurs activités dans des fichiers journaux. L'exhaustivité des informations varie en fonction du niveau de suivi librement personnalisable. Les fichiers journaux sont d'une grande utilité pour analyser les problèmes.

Le niveau de suivi est défini sur ERREUR par défaut. Si vous souhaitez obtenir plus d'informations de suivi, vous devez définir le niveau de suivi, sur DETAIL par exemple pour la fonction Software Delivery ou pour le service de transport de données. Vous devez, pour cela, exécuter l'*une* des commandes cftrace suivantes :

```
cftrace -c set -f USD -l DETAIL -s 30000
```

```
cftrace -c set -f DTS -l DETAIL -s 30000
```

L'option -s définit la taille du fichier journal sur 30 000 Ko. La taille par défaut est de 2 000 Ko, ce qui peut s'avérer insuffisant pour le niveau de suivi DETAIL. (Le fichier de suivi est écrasé, lorsque la taille limite et le nombre de fichiers de suivi configurés sont atteints).

Sur Windows, les fichiers journaux pour l'ensemble des services CAF sont situés sous *rép_installation*\logs (par défaut : c:\Program Files\CA\DSM\logs).

Les fichiers journaux créés au cours de l'installation de CA Client Automation se trouvent dans votre dossier temporaire d'utilisateur. En général, la variable d'environnement %temp% indique ce dossier.

Sur Linux, les fichiers journaux pour l'ensemble des services CAF sont situés sous $CA_DSM_BASEDIR/logs.

Les fichiers journaux créés au cours de l'installation de CA Client Automation se trouvent sous /opt/CA/installer/log.

Fichiers journaux de suivi

Les composants Client Automation produisent des fichiers journaux de suivi de leurs activités système pendant leur exécution. Vous pouvez les utiliser pour analyser et régler des problèmes.

Chaque processus Client Automation écrit les données dans son propre journal de suivi. Si le magasin de configurations contient une configuration de suivi pour un processus, le processus écrit les informations de suivi dans le fichier défini. Si le magasin de configurations ne contient aucune configuration de suivi pour un processus, le processus écrit les informations de suivi dans un fichier dont le nom est attribué en fonction du nom du processus. S'il existe plusieurs instances pour un même processus, vous pouvez définir chaque instance pour que l'écriture des données s'effectue dans le journal de suivi nommé de façon unique pour chacune d'entre elles. Toutefois, cette fonction est désactivée par défaut afin d'empêcher la création d'un grand nombre de fichiers de suivi. Vous pouvez activer cette fonction (via une configuration commune) lorsque vous souhaitez régler les problèmes liés au système.

Si le niveau de suivi d'un processus est défini sur ERREUR et qu'un suivi de niveau ERREUR est généré, Client Automation écrit les informations supplémentaires concernant le suivi de niveau INFORMATION dans le fichier journal de suivi. Ces informations supplémentaires de niveau INFORMATION offre davantage de données concernant le contexte de l'erreur et indiquent les suivis de niveau inférieur qui ont abouti à l'erreur.

Vous pouvez définir les paramètres de la fonction de suivi via la ligne de commande ccnfcmda.

Remarque : Pour plus d'informations sur la commande ccnfcmda de l'agent de configuration, saisissez <command> / ? dans l'invite de commande.

Outil de diagnostic dsminfo

CA Technologies propose l'outil dsmInfo qui collecte des informations de diagnostic à partir des systèmes sur lesquels est installé Client Automation. Les données collectées sont compressées dans un fichier unique qui contient des fichiers journaux, des informations système, des structures de répertoires et des informations de registre et d'environnement. Cet outil de diagnostic est disponible sur le support d'installation du produit de Client Automation, dans le dossier DiagnosticTools.

Si vous parvenez à reproduire un problème avec Client Automation, exécutez la commande suivante pour modifier le niveau de suivi sur DETAIL :

```
cftrace -c set -l DETAIL
```

Reproduisez le problème et collectez les informations de diagnostic à l'aide de l'outil dsmInfo.

Remarques :

Pour plus d'informations sur cet outil, consultez le fichier DSMInfoReadMe.txt disponible dans le dossier DiagnosticTools du support d'installation du produit.

Par défaut, l'outil dsmInfo produit des fichiers ".7z". Ces fichiers permettent une meilleure compression que les fichiers ZIP, ce qui facilite leur chargement dans CA Technologies.

Configuration commune

Client Automation est configuré de manière centralisée via un composant de configuration commun. Le composant de configuration commun fournit des fonctions permettant d'accéder à la configuration de Client Automation, de la stocker et de la gérer.

Paramètres de configuration

La plus petite unité de configuration est le paramètre. Les paramètres peuvent être regroupés en stratégies de configuration, que vous pouvez affecter à des ordinateurs ou à des groupes d'ordinateurs.

Dans le modèle de configuration, les objets suivants sont définis :

Paramètre

Contient des données de configuration. Un paramètre possède un nom et contient au moins une valeur.

Informations de paramètre

Contient des informations supplémentaires sur un paramètre.

Section des paramètres

Collection de paramètres qui sont logiquement liés. Par exemple, ils configurent des fonctionnalités liées. Les sections de paramètres sont utilisées pour établir la structure hiérarchique des ensembles de paramètres.

Stratégie de configuration

Collection de paramètres propres aux groupes ou aux ordinateurs.

Configuration

Représente l'état de configuration d'un ordinateur, puis est affectée à un ordinateur ou à un groupe d'ordinateurs. La valeur de la configuration peut être planifiée, programmée, active ou erronée.

Gestion des paramètres de configuration

La stratégie par défaut, qui correspond à l'ensemble des paramètres par défaut du gestionnaire, contient des paramètres destinés à la gestion à distance. La stratégie par défaut n'inclut pas les paramètres qui ne concernent que les applications locales de l'ordinateur.

Il existe deux types de mode de gestion des paramètres dans la stratégie par défaut : géré localement ou géré de manière centralisée. Le mode de gestion d'un paramètre peut être changé dans le gestionnaire uniquement.

- Les paramètres gérés localement sont contrôlés par des applications qui s'exécutent sur l'ordinateur local.
- Les paramètres gérés de manière centralisée sont contrôlés par l'intermédiaire de stratégies du gestionnaire et sont en lecture seule pour les applications locales. Les paramètres gérés de manière centralisée sont prioritaires par rapport aux paramètres gérés localement.

Certaines applications, telles qu'Contrôle distant, peuvent être installées en mode autonome. Une conséquence des installations autonomes est que leurs paramètres de configuration ne sont pas contrôlés par la stratégie par défaut du gestionnaire et que les valeurs de paramètre ne sont pas signalées au gestionnaire. Le mode autonome est prioritaire par rapport aux modes gérés localement et de manière centralisée. Vous pouvez définir le mode autonome au cours de l'installation de l'application, Contrôle distant, par exemple.

Stratégies de configuration

A des fins administratives, vous pouvez regrouper les paramètres dans des stratégies de configuration. Ces stratégies peuvent être affectées à des ordinateurs ou des groupes d'ordinateurs.

Un ordinateur ou un groupe d'ordinateurs peut également être soumis à plusieurs stratégies de configuration. Dans ce cas, la configuration des paramètres définie dans l'une des stratégies peut chevaucher les paramètres définis dans une autre stratégie. Afin de résoudre les conflits, vous devez respecter les indications suivantes lorsque des stratégies de configuration se chevauchent :

- Les stratégies affectées à un groupe sont héritées par l'enfant du groupe. Un enfant peut être un groupe ou un ordinateur.
- Dans une hiérarchie, les stratégies affectées au niveau enfant écrasent celles du niveau parent. Ainsi, tous les paramètres définis au niveau parent sont également définis pour l'enfant, mais une stratégie enfant sera prioritaire en cas de chevauchement avec une stratégie parent.

Rapport de configuration des agents

Dès que la configuration des paramètres d'un agent est modifiée, celui-ci rapporte les changements à son gestionnaire. Dans le gestionnaire, ces paramètres apparaissent dans l'explorateur DSM en tant que Configuration signalée.

Configuration de l'agent du gestionnaire d'entreprise

L'infrastructure CA Client Automation utilise une architecture et une méthodologie de configuration communes. L'administrateur se sert de l'interface de l'explorateur DSM pour apporter des modifications à la stratégie de configuration. Un gestionnaire de domaines se charge de stocker ces modifications dans la base de données de gestion (MDB). Ensuite, les modifications sont transmises à un agent qui les applique.

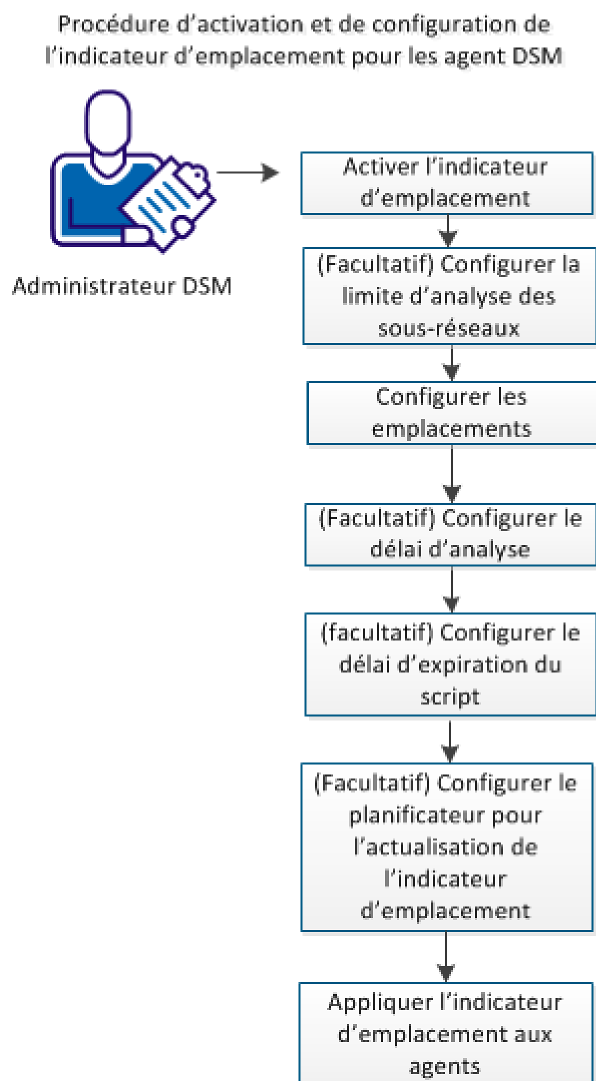
Dans tous les cas à l'exception d'un, il s'agit d'une solution simple. Cependant, en présence d'un gestionnaire d'entreprise, l'architecture de la gestion de configuration devient légèrement moins intuitive.

Pour prendre en charge une configuration gérée, un gestionnaire d'entreprise doit également être géré. Ceci nécessite l'installation d'un agent. Les agents communiquent avec des serveurs de modularité, qui eux-mêmes communiquent avec des gestionnaires de domaines. Vous devez définir quels serveurs de modularité et gestionnaires de domaines devront gérer l'ordinateur du gestionnaire d'entreprise.

La plupart des organisations ne déploient qu'un seul et unique gestionnaire d'entreprise.

Procédure d'activation et de configuration de l'indicateur d'emplacement

En tant qu'administrateur, la tâche de création de stratégie d'indicateur d'emplacement vous incombe. Vous pouvez configurer l'ordinateur de façon à ce qu'il informe un serveur de modularité approprié lorsqu'un changement d'emplacement est détecté. Vous pouvez appliquer la fonctionnalité d'indicateur d'emplacement à une stratégie sur les agents DSM pour permettre à l'ordinateur d'évaluer les règles de l'indicateur d'emplacement.



Procédez comme suit :

1. Activez l'indicateur d'emplacement (page 59).
2. (Facultatif) Configurez la limite de l'analyse des sous-réseaux (page 60).
3. Configurez des emplacements (page 61).
4. (Facultatif) Configurez le délai d'attente de l'analyse (page 68).
5. (Facultatif) Configurez le délai d'expiration du script (page 68).
6. (Facultatif) Configurez le planificateur pour l'actualisation de l'indicateur d'emplacement (page 69).
7. Appliquez l'indicateur d'emplacement aux agents (page 71).

Activation de l'indicateur d'emplacement

La fonctionnalité d'indicateur d'emplacement n'est pas activée par défaut pour une nouvelle installation ou une mise à niveau. L'activation de la stratégie d'indicateur d'emplacement vous permet de détecter les modifications apportées à l'emplacement géographique d'un agent. Lorsqu'une modification est détectée, l'agent évalue les règles, puis se connecte au serveur de modularité approprié.

Important : Avant d'activer la fonctionnalité d'indicateur d'emplacement, désactivez toutes les autres solutions d'indicateur d'emplacement présentent dans l'environnement CA ITCM.

Procédez comme suit:

1. Accédez à DSM, Agent, Agent commun, Standard, Indicateur d'emplacement.

   Les paramètres de l'indicateur d'emplacement suivants sont affichés.

   - Activé
   - Limiter l'analyse des sous-réseaux
   - Emplacements
   - Délai d'attente de l'analyse
   - Temporisation de script

2. Sélectionnez Activé, puis cliquez sur Définition des paramètres dans le portlet Tâches.

   La boîte de dialogue Définition des propriétés s'ouvre.

3. Dans le champ Valeur, sélectionnez True, puis cliquez sur OK.

   La fonctionnalité est activée dans la stratégie. La stratégie est activée uniquement lorsque vous la scellez et l'appliquez à un agent.

Remarque :

- Si l'agent est exécuté sur le même ordinateur qu'un serveur de modularité, la stratégie d'indicateur d'emplacement est toujours désactivée.
- Si le serveur de modularité d'agent est marqué comme géré de façon centralisée, la fonctionnalité d'indicateur d'emplacement de l'agent ne peut pas modifier la valeur après l'évaluation des règles.

(Facultatif) Configuration de la limite de l'analyse des sous-réseaux

Vous pouvez configurer la limite de l'analyse des sous-réseaux pour permettre ou empêcher l'analyse des sous-réseaux pour rechercher des serveurs de modularité dans d'autres domaines.

Procédez comme suit:

1. Accédez à la stratégie de configuration de l'indicateur d'emplacement.

   Les paramètres de l'indicateur d'emplacement sont affichés dans le volet droit.

2. Double-cliquez sur Limiter l'analyse des sous-réseaux.
3. Cliquez sur Définition des propriétés dans le portlet Tâches.

   La boîte de dialogue Définition des propriétés s'ouvre.

4. Modifiez le champ Valeur de manière appropriée à votre environnement.

   Valeur par défaut : True

5. Cliquez sur OK.

   Le paramètre Limiter l'analyse des sous-réseaux est configuré.

Configuration des emplacements

Définissez les règles d'emplacement pour prendre en charge les modifications d'emplacement géographique et permettre aux agents de se connecter aux serveurs de modularité appropriés. Les agents évaluent les règles que vous créez pour déterminer le serveur de modularité auquel se connecter.

Procédez comme suit:

1. Sélectionnez Emplacements, puis cliquez sur Définition des paramètres dans le portlet Tâches.

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Cliquez sur Ajouter une ligne pour configurer les règles.

   La fonctionnalité ajoute une ligne contenant les paramètres suivants à la structure de table actuelle :

   - Nom du lieu
   - Priorité
   - Address Range (Plage d'adresses)
   - Serveur de modularité.
   - Subnet Scan (Analyse de sous-réseau)
   - Script

3. Configurez chaque paramètre, puis cliquez sur OK.

   Les paramètres d'emplacement sont configurés.

Important : La plage d'adresses n'est pas vérifiée et le nom de serveur, l'analyse de sous-réseau et le script ne sont pas validés. Soyez prudent lorsque vous définissez ces paramètres.

Configuration de la priorité des règles d'emplacement

Vous pouvez spécifier la priorité du traitement des règles d'emplacement. L'agent évalue les règles et utilise la priorité spécifiée pour déterminer la règle à appliquer.

Par exemple, vous créez deux règles, règle A et règle B. Vous configurez la règle A avec une priorité 1 et la règle B avec une priorité 2. Si vous configurez tous les autres paramètres avec les mêmes valeurs pour la règle A et la règle B, l'agent obtient deux correspondances. Toutefois, la règle A est appliquée, car elle dispose de la priorité la plus élevée.

Procédez comme suit:

1. Double-cliquez sur la nouvelle valeur sous Priorité.

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Dans le champ Valeur, spécifiez la priorité pour la règle d'emplacement, puis cliquez sur OK.

   Priorité maximale : 0

   Priorité minimale : 99999

   La priorité de la règle d'emplacement est configurée.

Configuration de la plage d'adresses pour les règles d'emplacement

Si l'adresse de l'agent correspond aux critères de plage d'adresses IP, la règle d'emplacement est incluse dans la sélection. La fonctionnalité d'indicateur d'emplacement prend en charge les adresses IPv4 et IPv6. Lorsque l'agent obtient plusieurs règles correspondantes, la priorité des règles sert à déterminer le serveur à utiliser.

Procédez comme suit:

1. Double-cliquez sur la nouvelle valeur dans la colonne Address Range (Plage d'adresses).

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Entrez la plage d'adresses dans le champ Valeur, puis cliquez sur OK.

   Limites : La valeur minimum est de 1 caractère.

   Si vous utilisez des adresses IPv4, vous pouvez spécifier l'adresse IP, un caractère générique IP ou la plage d'adresses IP dans la colonne de plage d'adresses. Par exemple :

   - **Format d'adresse IP :** 192.168.1.1
   - **Format de caractère générique IP :** 192.168.1.*
   - **Format de plage d'adresses IP :** 192.168.2.1-192.168.2.100

   Si vous utilisez des adresses IPv6, vous pouvez spécifier les différents préfixes de ces adresses dans la colonne de plage d'adresses. Par exemple :

   2001:DB8::/48

   Identifie l'organisation, le site, le sous-site et le sous-réseau. La longueur du préfixe en bits est 48 et le nombre maximum de bits permis est 64.

   Préfixes d'adresses spéciales :

   FE80::/64

   Utilisé pour la mise en correspondance d'un préfixe local de lien, c'est-à-dire, un sous-réseau local.

   FEC0::/64

   Utilisé pour la mise en correspondance d'un préfixe local de site.

   ::/0

   Utilisé pour la mise en correspondance de toutes les adresses IPv6.

   Adresses de groupe de multidiffusion :

   FF02::1

   Utilisé pour la mise en correspondance de tous les noeuds sur le segment de réseau local (lien-local).

   FF05::1

Utilisé pour la mise en correspondance de tous les noeuds sur le réseau du site (site-local).

FF08::1

Utilisé pour la mise en correspondance de tous les noeuds sur le réseau de l'organisation (organisation-local).

La plage d'adresses pour la règle d'emplacement est configurée.

Configuration du serveur de modularité pour les règles d'emplacement

Les valeurs de la colonne Serveur de modularité vous permettent de définir le nom de domaine complet des adresses IP d'un serveur de modularité auquel l'agent se connecte.

Procédez comme suit:

1. Double-cliquez sur la nouvelle valeur sous Serveur de modularité.

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Entrez l'adresse IP ou le nom de domaine complet du serveur de modularité auquel se connecte l'agent qui réside dans la plage d'adresses.

   Le serveur de modularité pour la règle d'emplacement est configuré.

Remarque : Si vous spécifiez le serveur de modularité, laissez les colonnes Subnet Scan (Analyse de sous-réseau) et Script vides. Si vous n'utilisez pas le serveur de modularité, laissez la colonne Serveur de modularité vide.

Configuration de l'analyse de sous-réseau pour les règles d'emplacement

La configuration de l'analyse de sous-réseau définit la règle permettant d'analyser le sous-réseau spécifié et détecte les serveurs de modularité actifs sur ce sous-réseau. L'agent évalue les autres règles et les délais de réponse estimés des serveurs actifs afin de sélectionner le meilleur serveur. La fonctionnalité d'indicateur d'emplacement prend en charge les adresses IPv4 et IPv6.

Procédez comme suit:

1. Double-cliquez sur la nouvelle valeur dans la colonne Subnet Scan (Analyse de sous-réseau).

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Entrez une valeur pour l'analyse de sous-réseau dans le champ Valeur, puis cliquez sur OK.

   Si vous utilisez des adresses IPv4, vous pouvez spécifier l'adresse IP, un caractère générique IP ou la plage d'adresses IP dans la colonne Subnet Scan (Analyse de sous-réseau).

   Si vous utilisez des adresses IPv6, vous pouvez spécifier les différents préfixes de ces adresses dans cette colonne.

   L'analyse de sous-réseau pour la règle d'emplacement est configurée.

Remarque : Si vous spécifiez l'analyse de sous-réseau, laissez les colonnes Serveur de modularité et Script vides. Si vous n'utilisez pas l'analyse de sous-réseau, laissez la colonne Subnet Scan (Analyse de sous-réseau) vide.

Configuration de script pour les règles d'emplacement

Vous pouvez ajouter un script à exécuter sur l'agent pour déterminer le serveur de modularité à utiliser. Vous devez livrer ce script à l'agent.

Procédez comme suit:

1. Double-cliquez sur la nouvelle valeur dans la colonne Script.

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Dans le champ Valeur, spécifiez le nom du script du gestionnaire de domaines, puis cliquez sur OK.

   Remarque : Vous pouvez spécifier l'emplacement de script comme un chemin d'accès absolu ou relatif. Un chemin d'accès relatif dépend du répertoire d'installation de CA ITCM, qui se trouve généralement à l'un des emplacements suivants :

   Windows :

   C:\Program Files(x86)\CA\DSM

   UNIX, Linux :

   /opt/CA/DSM

   Les paramètres suivants sont transférés au script de sélection de serveur :

   -o <nom_fichier_sortie>

   Nom du fichier dans lequel le script écrit le nom du serveur de modularité qu'il identifie.

   -x <nom_fichier_erreur>

   Nom du fichier dans lequel le script écrit toutes les informations d'erreur qu'il génère.

   -un <adresse_correspondante>

   Identifie l'adresse correspondante et le script est exécuté.

   Le script du gestionnaire de domaines est configuré pour la règle d'emplacement.

   Remarque : Si vous spécifiez le script, laissez les colonnes Serveur de modularité et Subnet Scan (Analyse de sous-réseau) vides. Si vous n'utilisez pas l'analyse de sous-réseau, laissez la colonne Subnet Scan (Analyse de sous-réseau) vide.

Exemple :

```
rem -------------------------------------------------------------------
rem Script simple d'identification de serveur avec indicateur
d'emplacement
rem Ce script écrit un nom de serveur codé de manière irréversible dans
le fichier de sortie.
rem -------------------------------------------------------------------
```

```
dim sMatchingAddress as string
dim sOutputFileName as string
dim sErrorFileName as string

dim X as Integer
FOR X=0 to argc()

        rem Lit le fichier de sortie à partir des paramètres fournis.

        if ( argv(X)="-o") THEN
        sOutputFileName = argv(X+1)
        ENDIF

        rem Lit l'adresse correspondante à partir des paramètres fournis.

    if ( argv(X)="-a") THEN
        sMatchingAddress = argv(X+1)
        ENDIF

        rem Lit l'adresse correspondante à partir des paramètres fournis.

        if ( argv(X)="-x") THEN
        sErrorFileName = argv(X+1)
        ENDIF

NEXT X

dim fHandle as integer

fHandle = OpenFile(sOutputFileName,O_WRITE)
IF NOT(EOF(fHandle)) Then
        WriteFile(fHandle,"sampleserver.ca.com")
        CloseFile(fHandle)
        exit
ENDIF
exit
```

(Facultatif) Configuration du délai d'attente de l'analyse

Si vous utilisez l'analyse de sous-réseau, la configuration du délai d'attente de l'analyse détermine le délai d'attente maximum d'une réponse d'un serveur de modularité.

Procédez comme suit:

1. Double-cliquez sur Configure Scan Timeout (Configurer le délai d'attente de l'analyse), puis cliquez sur Définition des propriétés dans le portlet Tâches.

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Modifiez le champ Valeur de manière appropriée à votre environnement, puis cliquez sur OK.

   Valeur par défaut : 30

   Le paramètre Configure Scan Timeout (Configurer le délai d'attente de l'analyse) est configuré.

(Facultatif) Configuration du délai d'expiration du script

La configuration du délai d'expiration du script détermine l'intervalle maximum pendant lequel exécuter le script. L'exécution des scripts s'arrête lorsque le délai spécifié est écoulé.

Procédez comme suit:

1. Sélectionnez Délai d'expiration du script, puis cliquez sur Définition des paramètres dans le portlet Tâches.

   La boîte de dialogue Définition des propriétés s'ouvre.

2. Modifiez le champ Valeur de manière appropriée à votre environnement, puis cliquez sur OK.

   Valeurs :

   - **0 :** délai d'expiration infini
   - **> 0 :** nombre de secondes pour l'exécution du script avant l'expiration
   - **Valeur maximum du délai d'expiration permise :** 600 secondes (10 minutes)

   Valeur par défaut : 300

   Le paramètre Délai d'expiration du script est configuré.

(Facultatif) Configuration du planificateur pour l'actualisation de l'indicateur d'emplacement

Le dossier du groupe de stratégies Actualiser l'indicateur d'emplacement contient un job qui enregistre CAF auprès du serveur à intervalles réguliers. Pour modifier un paramètre de stratégie, double-cliquez sur une stratégie pour afficher la boîte de dialogue Définition des propriétés.

Planificateur CAF : ligne de commande

Définit la commande CAF qui exécute ce job.

Valeur par défaut : location aware

Planificateur CAF : jours à exclure

Répertorie les jours à exclure de la planification. Spécifiez une combinaison au choix des valeurs suivantes : Lundi, Mardi, Mercredi, Jeudi, Vendredi, Samedi et Dimanche. Séparez les valeurs par des virgules.

Valeur par défaut : vide

Planificateur CAF : activé

Indique si le job d'actualisation de l'enregistrement est activé.

Valeur par défaut : True

Planificateur CAF : heure

Pour les planifications quotidiennes, définit l'heure à laquelle exécuter le job. Cette stratégie n'est pas utilisée pour les planifications horaires et à la minute.

Valeur par défaut : 12

Planificateur CAF : heures à exclure

Répertorie les heures à exclure de la planification. Spécifiez les heures, au format 24 heures. Séparez les valeurs par des virgules.

Valeur par défaut : vide

Planificateur CAF : minute

Pour les planifications quotidiennes, définit les minutes après l'heure à laquelle exécuter le job. Cette stratégie n'est pas utilisée pour les jobs à la minute.

Valeur par défaut : 0

Planificateur CAF : minutes aléatoires

Définit le nombre de minutes ajoutées à un job random_minute. Le job s'exécute à l'heure spécifiée plus un nombre aléatoire de minutes jusqu'à la valeur définie. La stratégie exécute les intervalles réguliers et approximatifs d'un job afin de répartir la charge de serveur en rendant le contact des agents partiellement aléatoire.

Valeur par défaut : 90

Planificateur CAF : heure aléatoire

Spécifie le temps en secondes durant lequel un job random_now est lancé. Le job s'exécute au cours d'un nombre aléatoire de secondes jusqu'à la valeur spécifiée. Cette stratégie garantit que les ordinateurs qui démarrent ensemble n'initialisent pas leurs jobs simultanément.

Valeur par défaut : 0

Planificateur CAF: nombre de répétitions

Indique l'intervalle entre les répétitions du job. Cette valeur dépend du type de job. Par exemple, si le type est jour, cette valeur représente le nombre de jours entre les jobs.

Valeur par défaut : 1

Planificateur CAF : type de job

Spécifie le type d'intervalle de planification. Les valeurs valides sont le jour, l'heure et la minute. Vous pouvez également ajouter les qualificatifs facultatifs suivants :

random

Exécute le job avec un temps quelconque ajouté à l'heure du job spécifié, jusqu'à la valeur des minutes aléatoires.

random_hour

S'exécute à une heure quelconque du jour.

random_minute

S'exécute à une minute quelconque de l'heure.

maintenant

Démarre le job immédiatement après l'heure du job spécifié.

Séparez les valeurs par des virgules.

Exemples :

Exécutez le job amagent tous les jours à 14 h 30 :

```
type="day", repeat=1, hour=14, minute=30, cmd="start
amagent"
```

Exécutez le job amagent lorsque CAF démarre et tous les jours par la suite (sauf les week-ends) à une heure aléatoire comprise entre 01 h 00 et 02 h 30 :

```
type="day now random", hour=1, minute=0, randomminutes=90,
excludedays="Saturday Sunday", cmd="start amagent"
```

Application de l'indicateur d'emplacement aux agents

Après la création et le scellement d'une nouvelle stratégie, appliquez-la à un actif, à savoir, un ordinateur ou un groupe.

Pour un actif, procédez comme suit :

1. Accéder au dossier Stratégies de configuration sous le nœud du Panneau de configuration dans l'arborescence.
2. Cliquez avec le bouton droit de la souris sur la stratégie à appliquer, puis sélectionnez Copier dans le menu contextuel.
3. Dans l'arborescence, accédez à l'actif approprié, cliquez dessus avec le bouton droit de la souris et sélectionnez Coller dans le menu contextuel.

   La stratégie est appliquée à l'actif.

Pour plusieurs actifs ou groupes, procédez comme suit :

1. Dans l'arborescence, sélectionnez les actifs ou groupes.
2. Cliquez avec le bouton droit de la souris sur les cibles sélectionnées, puis sélectionnez Coller dans le menu contextuel.

   Un autre menu contextuel s'ouvre.
3. Cliquez sur Stratégies de configuration.

   La boîte de dialogue Planifier les stratégies s'ouvre.
4. Planifiez la stratégie à activer.

   Remarque : Lorsque vous appliquez des stratégies à un actif ou à un groupe unique, le bouton Personnaliser et prévisualiser est activé. Il est désactivé lorsque vous collez une stratégie pour plusieurs actifs ou groupes.
5. Cliquez sur OK pour appliquer la stratégie à plusieurs actifs ou groupes.

Vous avez activé et configuré la fonctionnalité d'indicateur d'emplacement pour les agents DSM.

Environnements d'exploitation pris en charge

CA Client Automation (Client Automation) prend en charge les principaux environnements d'exploitation. Pour obtenir la liste actuelle des plates-formes prises en charge, consultez la matrice de compatibilité.

Remarque : Dans ce document, le terme UNIX fait référence aux systèmes d'exploitation dérivés d'UNIX : AIX, HP-UX, Solaris et Mac OS X. Si un composant système ou une fonctionnalité logicielle de cette version ne s'applique pas à tous les dérivés d'UNIX, cela est clairement indiqué dans la description du composant ou de la fonctionnalité concernée.

Spécifications matérielles et configuration requise

Les tableaux ci-dessous répertorient les spécifications matérielles et la configuration requise recommandées pour cette version.

La configuration matérielle requise réelle varie selon la charge du système, notamment la fréquence et le nombre des opérations de collecte et de transfert de données ainsi que la quantité de données collectées et transférées.

Spécifications du gestionnaire d'entreprise

Un gestionnaire d'entreprise DSM requiert (au moins) la configuration matérielle suivante :

Composant	**Vitesse/Taille**
Lecteur de DVD-ROM	Non spécifié(e)
UC	1 ou 2 unités centrales de 2 GHz **Remarque :** 2 unités centrales sont requises si la MDB est hébergée sur le même ordinateur que le gestionnaire d'entreprise DSM.
Mémoire	2 Go minimum **Remarque :** Une mémoire RAM d'au moins 4 Go est requise si la MDB est hébergée sur le même ordinateur que le gestionnaire d'entreprise DSM.
Espace disque	30 Go minimum **Remarque :** Un espace libre d'au moins 100 Go est requis si la MDB est hébergée sur le même ordinateur que le gestionnaire d'entreprise DSM. **Important :** La partition de disque sur laquelle se trouve la MDB doit inclure l'espace nécessaire. Prévoyez de l'espace supplémentaire pour la bibliothèque de packages logiciels. L'espace total nécessaire dépend du nombre et de la taille des packages à stocker.
Carte réseau	100 Mbits/s

Spécifications du gestionnaire de domaines

Un gestionnaire de domaines DSM requiert (au moins) la configuration matérielle suivante :

Composant	Vitesse/Taille
Lecteur de DVD-ROM	Non spécifié(e)
UC	1 ou 2 unités centrales de 2 GHz **Remarque :** 2 unités centrales sont requises si la MDB est hébergée sur le même ordinateur que le gestionnaire de domaines DSM.
Mémoire	2 Go minimum **Remarque :** Une mémoire RAM d'au moins 4 Go est requise si la MDB est hébergée sur le même ordinateur que le gestionnaire de domaines DSM.
Espace disque	30 Go minimum **Remarque :** Un espace libre d'au moins 100 Go est requis si la MDB est hébergée sur le même ordinateur que le gestionnaire de domaines DSM. **Important :** La partition de disque sur laquelle se trouve la MDB doit inclure l'espace nécessaire. Prévoyez de l'espace supplémentaire pour la bibliothèque de packages logiciels. L'espace total nécessaire dépend du nombre et de la taille des packages à stocker.
Carte réseau	100 Mbits/s

Spécifications du serveur de modularité

Un serveur de modularité DSM requiert (au moins) la configuration matérielle suivante :

Remarque : Cette configuration minimum s'applique à tous les environnements d'exploitation Windows, RedHat et SuSE pris en charge.

Composant	Vitesse/Taille
UC	1 unité centrale de 2 GHz
Mémoire	2 Go
Espace disque	30 Go
Carte réseau	100 Mbits/s

Spécifications de l'agent

Un agent DSM requiert (au moins) la configuration matérielle suivante :

Remarque : Cette configuration minimum s'applique à tous les environnements d'agent pris en charge.

Composant	Vitesse/Taille
UC	1 unité centrale de 2 GHz
Mémoire	256 Mo
Espace disque	300 Mo
Carte réseau	10 Mbits/s

Spécifications de l'explorateur DSM

L'explorateur DSM requiert (au moins) la configuration matérielle suivante :

Remarque : Cette configuration minimum s'applique uniquement aux environnements d'exploitation Windows pris en charge.

Composant	Vitesse/Taille
Lecteur de DVD-ROM	Non spécifié(e)
UC	1 unité centrale de 2 GHz
Mémoire	2 Go
Espace disque	30 Go
Carte réseau	100 Mbits/s
Carte graphique	Résolution de 1024x768

Spécifications pour une MDB SQL Server sous Windows

Une base de données de gestion (MDB) Microsoft SQL Server sous Windows requiert (au moins) la configuration matérielle suivante :

Composant	Vitesse/Taille
Lecteur de DVD-ROM	Non spécifié(e)
UC	2 unités centrales de 2 GHz
Mémoire	4 Go
Espace disque	100 Go

Composant	Vitesse/Taille
Carte réseau	100 Mbits/s

Spécifications relatives à une MDB Oracle

L'installation de plusieurs instances de MDB Oracle requiert (au moins) la configuration matérielle suivante :

Composant	Vitesse/Taille
Lecteur de DVD-ROM	Non spécifié(e)
UC	2 unités centrales de 1,5 GHz
Mémoire	Prévoyez au moins 3,2 Go de mémoire principale (2,7 Go pour la zone SGA et 0,5 Go pour la zone PGA) pour chaque instance de base de données Oracle configurée. **Remarque :** Cette configuration est conseillée pour une installation comprenant jusqu'à 10 000 actifs informatiques.
Espace disque	100 Go
Carte réseau	100 Mbits/s

Inventaire et gestion des unités

Les fonctions Asset Management dans CA Client Automation (Client Automation) offrent aux administrateurs un mécanisme automatisé simple pour inventorier et gérer les unités présentes sur un réseau d'entreprise, via un processus de détection et de déploiement d'agent. Le fait qu'un agent soit installé sur les unités détectées permet une gestion et un contrôle permanents centralisés des unités.

Cette section fournit des informations sur les fonctionnalités Asset Management suivantes :

- Composant de l'inventaire standard (page 76)
- Prise en charge de l'inventaire des non-résidents (page 76)

Pour plus d'informations sur les fonctions, composants et exigences d'Asset Management, consultez le *manuel d'administration d'Asset Management*, disponible dans la documentation CA Client Automation.

Composant de l'inventaire standard

Le composant de l'inventaire de base détecte un sous-ensemble dynamique d'informations matérielles sur l'ordinateur local et les met à disposition des autres composants DSM. Le détail des informations d'inventaire dépend de l'environnement matériel et de la plate-forme sur lesquels il s'exécute.

Les informations de l'inventaire standard comportent les informations matérielles suivantes :

- Système (par exemple, Balise d'actif, Modèle, Processeurs ou Mémoire)
- Système d'exploitation (par exemple Langue, Système d'exploitation, Service pack ou Version)
- Unités système (par exemple Adaptateurs réseau ou vidéo)
- Réseau (par exemple Nom de l'ordinateur et du domaine, Adresse IP / IPv6 ou TCP/IP)
- Systèmes de fichiers (par exemple Systèmes de fichier locaux ou partitionnement)
- Etat du système (par exemple Dernière analyse matérielle)

Remarque : Quelle que soit la langue dans laquelle CA Client Automation est exécuté, ces informations d'inventaire sont toujours disponibles en anglais.

Prise en charge d'inventaires non-résidents

La fonction de prise en charge d'inventaires non-résidents (NRI) d'Asset Management complète la fonction d'inventaire en permettant aux administrateurs d'entreprise d'inventorier leurs réseaux sans avoir un impact permanent sur les unités inventoriées. Le NRI offre une solution élective vers laquelle les utilisateurs finaux sont dirigés lorsqu'ils utilisent une page Web pour collecter l'inventaire de leur système, mais également une solution gérée dans laquelle l'administrateur d'entreprise lance une collecte d'inventaire, par exemple via des scripts de connexion.

La prise en charge NRI utilise des composants de l'agent DSM normal combinés au collecteur de ressources et à la console Web.

Pour pouvoir utiliser le NRI, au moins une console Web (et les Services Web associés) et un collecteur de ressources doivent être installés pour chaque gestionnaire de domaine devant collecter et stocker un inventaire non-résident. Dans le scénario le plus simple, chaque gestionnaire de domaine peut co-héberger une console Web et un collecteur de ressources unique. Pour des scénarios plus complexes et évolutifs, un certain nombre de serveurs de modularité peuvent co-héberger des consoles Web et des collecteurs de ressources.

Le NRI est installé de manière intégrée à la fonction Asset Management via le programme d'installation de CA Client Automation. Le NRI est configuré à l'aide d'un fichier de configuration simple (fichier script).

NRI prend en charge l'inventaire sur des ordinateurs cibles Windows, Linux ou UNIX. De même, les composants de gestion de le NRI sont uniquement pris en charge sur les gestionnaires et serveurs de modularité exécutant Windows.

Limitations de NRI

Si vous exécutez NRI avec un compte d'utilisateur de domaine standard disposant de moins de droits que l'utilisateur racine (sous UNIX et Linux) ou un compte d'administrateur (sous Windows), les rapports d'inventaire de l'agent NRI seront moins nombreux que pour l'agent régulier Client Automation.

L'agent NRI collecte autant d'informations que possible en fonction des droits avec lesquels il est exécuté.

Remarque : Pour plus d'informations sur NRI, consultez le *Manuel d'administration d'Asset Management*.

Chapitre 2: Planification de l'implémentation d'infrastructure

Ce chapitre contient des informations importantes sur les exigences et la modularité de CA Client Automation. Ces informations doivent être lues et comprises avant le déploiement de tout composant DSM.

Ce chapitre traite des sujets suivants :

Prise en charge d'IPv6

IPv6 (Internet Protocol version 6) est après IPv4 la seconde version du protocole Internet officiellement adoptée pour un usage général. IPv6 est destiné à offrir plus d'adresses pour les unités réseau, en permettant par exemple à chaque téléphone cellulaire et à chaque appareil électronique mobile de disposer de sa propre adresse.

IPv6 fonctionne sur la base d'adresses 128 bits et propose donc un espace d'adresses très important. Ce vaste espace d'adresses permet de disposer d'un nombre quasi-illimité de hiérarchies et d'affectations d'adresses à des domaines particuliers. Il améliore également la configuration automatique, la sécurité, le routage simplifié, ainsi que d'autres services.

Client Automation est compatible avec IPv6 et peut fonctionner dans des environnements IPv4 purs, IPv6 purs ou IPv4/IPv6 mixtes.

Avec IPv6, les cartes réseau peuvent disposer de plusieurs adresses IPv6 et disposer également à la fois d'adresses IPv4 et IPv6. Nous vous recommandons vivement d'utiliser des noms de domaine complets (FQDN) pour identifier les gestionnaires, les serveurs de modularité, etc.

Restrictions dans le cadre de la prise en charge IPv6

Les restrictions suivantes s'appliquent dans le cadre de la prise en charge IPv6 dans CA Client Automation (Client Automation) :

- Si vous avez défini le paramètre protocolprecedence dans comstore sur ipv6,ipv4 et si vous utilisez une MDB Oracle, vous constaterez que le produit fonctionne lentement. Cela est dû au fait que les connexions à la base de données essaient d'abord les adresses IPv6, qui ne parviennent pas établir la connexion avec la base de données Oracle, avant d'essayer une adresse IPv4. Afin d'éviter cette dégradation des performances, tout en continuant à utiliser de préférence les adresses IPv6 dans d'autres parties du produit, veuillez créer dans le registre le DWORD suivant avec une valeur de 1, HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Unicenter ITRM\UseIPv4ForDB.
- La gestion des installations de SE (OSIM) est uniquement disponible dans les réseaux prenant en charge IPv4. Cela est dû au fait que OSIM s'appuie sur le système PXE qui s'appuie lui-même sur IPv4.
- Client Automation ne prend pas en charge les adresses locales de lien lors de la mise en contact avec les composants d'infrastructure, à l'exception des deux cas suivants :
  - Lors de la connexion d'une visionneuse Remote Control à un hôte Remote Control, une adresse locale de lien peut être saisie dans la visionneuse Remote Control.
  - Lors de l'utilisation de Remote Control pour parcourir le réseau local, des adresses locales de lien s'affichent et peuvent être sélectionnées.

  Remarque : Les adresses locales de lien sont collectées et affichées dans Collecte d'inventaire et Affichage.
- La méthode de téléchargement NOS pour un job Software Delivery (SD) n'est pas prise en charge sur un réseau purement IPv6 sous les conditions suivantes :
  - L'agent de la plate-forme utilise Samba ou NFS
  - L'agent est une plate-forme Windows antérieure à Windows Vista et utilise Microsoft NOS

Toutefois, si la plate-forme Windows est Windows Server 2003, les étapes suivantes peuvent être entreprises pour activer le téléchargement NOS :

1. La clé de registre suivante doit être définie sur 1 sur les ordinateurs équipés de l'agent :

   HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)

2. Les deux mises à jours correctives répertoriées ci-dessous doivent être appliquées à tous les ordinateurs équipés de l'agent qui souhaitent créer un partage de bibliothèque de serveur de modularité DSM :

   http://support.microsoft.com/kb/947369/en-us

   http://support.microsoft.com/kb/950092/en-us

3. Le nom d'hôte de l'ordinateur du serveur de modularité doit correspondre à une adresse IPv6 globale.

4. Le partage de la bibliothèque du serveur de modularité (conservé dans le comstore du serveur de modularité) doit utiliser un nom d'hôte (et non une adresse IP). Pour vérifier si une adresse IP est utilisée, exécutez les commandes suivantes :

   ```
   ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn exportarchive
   ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
   ```

   Si l'une des deux commandes renvoie une valeur intégrant une adresse IP, remplacez l'adresse par un nom d'hôte à l'aide des commandes suivantes :

   ```
   ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn exportarchive
   -v IP_remplacé_par_nom_hôte
   ```

   ```
   ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
   -v IP_remplacé_par_nom_hôte
   ```

   Par exemple, si GetParameterValue pour msiadminpathunc a renvoyé \\2001:db9:1:2:f045:c89:5c2:bdf5\SDMSILIB, la nouvelle valeur sera \\foobar.testarea.ca.com\SDMSILIB.

   Remarque : Pour plus d'informations sur la commande ccnfcmda de l'agent de configuration, saisissez <command> / ? dans l'invite de commande.

En pratique, si la méthode de téléchargement NOS ci-dessus échoue, Software Delivery aura recours à la méthode de téléchargement sans NOS. Toutefois, si la solution de secours est désactivée lors de la modification de la stratégie par défaut, le job SD échouera.

- L'appartenance aux conteneurs dynamiques de service de transport de données (DTS) WorldView prend uniquement en charge les plages d'adresses IPv4.

- Le déploiement de l'infrastructure et la détection continue prennent uniquement en charge les plages d'adresses IPv4.
- L'assistant Ordinateurs non gérés, qui permet à l'utilisateur de saisir un ou plusieurs sous-réseaux utilisés pour filtrer les ordinateurs non gérés, prend uniquement en charge les sous-réseaux IPv4.
- Le localisateur du service CAF fonctionne uniquement dans un sous-réseau local, ce qui risque d'affecter l'outil de packaging qui détectera les gestionnaires uniquement dans le sous-réseau local. (Cela varie si les routeurs acceptent la multidiffusion avec étendue.)
- Le protocole DTS PPP ne prend pas en charge IPv6.
- Client Automation ne prend pas en charge la désactivation d'IPv4 sur Windows Server 2003 et Windows XP, car la désactivation d'IPv4 sur ces plates-formes Windows n'est généralement pas prise en charge.
- Sous Windows Vista et Windows Server 2008, Client Automation prend en charge IPv6 pur. IPv4 doit être supprimé de ces plates-formes en saisissant la commande suivante dans une invite de commande :

  ```
  netsh interface ipv4 uninstall
  ```

  Un message s'affiche si un redémarrage est requis.

Remarques relatives à la configuration dans le cadre de la prise en charge IPv6

Dans le cadre de la prise en charge IPv6 dans CA Client Automation (Client Automation), vous devez tenir compte des remarques et aspects suivants en matière de configuration.

- Les paramètres de configuration (saisies de stratégie) dans l'explorateur DSM contrôlent les connexions IPv6 et IPv4 de la manière suivante :

  Définir l'ordre de priorité des recherches DNS

  Définit la priorité des requêtes DNS lors de l'exécution directe de requêtes DNS, c'est-à-dire sans utiliser les fonctions communes. Dans les environnement d'exploitation antérieurs à Windows Vista, le DNS est uniquement pris en charge sur IPv4.

  Valeur par défaut : ipv4, ipv6

Définir la priorité des résolutions de nom

Définir l'ordre de priorité des fonctions de résolution de nom. Dans certains environnements, la résolution de nom WINS et NETBIOS peut s'avérer plus fiable que le DNS. Dans certains cas, vous pouvez indiquer que la résolution NETBIOS doit être utilisée en priorité par rapport aux recherches DNS.

Si ce paramètre est configuré, la valeur du paramètre de configuration Utiliser les noms courts NETBIOS comme solution de secours est ignorée et la résolution de nom effectuera d'abord une requête NETBIOS en réduisant le nom de domaine complet à un nom court avant de recourir au DNS et à d'autres méthodes. Si une recherche de nom court initiée par cette stratégie a déjà été exécutée, la solution de secours des noms courts sera ignorée si elle activée. Ce paramètre est uniquement pris en charge par les systèmes Client Automation qui prennent en charge les recherches NETBIOS.

Remarque : Ce paramètre n'est actuellement pas utilisé.

Valeur par défaut : dns, netbios

Définir l'ordre de priorité des adresses résolues

Définit la priorité de la famille d'adresses IP (IPv6 ou IPv4) lorsque plusieurs familles d'adresses IP sont utilisées.

Lors de la résolution des adresses, ce paramètre géré de manière centralisée indique l'ordre de priorité à appliquer à chaque famille d'adresses. Par défaut, les adresses IPv4 sont résolues avant les adresses IPv6 afin de conserver une interopérabilité maximale.

Valeur par défaut : ipv4, ipv6

Activer la résolution IPv4

Active la prise en charge de la résolution d'adresse Ipv4. Ce paramètre est uniquement un espace réservé dans la version actuelle du logiciel. Les noeuds terminaux ignoreront donc le paramètre et prendront toujours en charge la résolution IPv4.

Valeur par défaut : True

Activer la résolution IPv6

Active la prise en charge de la résolution d'adresse IPv6, autorisant ainsi le retour des adresses IPv6. Si ce paramètre est désactivé (False), l'opérateur supprime toutes les adresses IPv6 des résultats de la résolution de nom.

Remarque : Ce paramètre est respecté par les noeuds terminaux, à la différence du contrôle IPv4 en miroir.

Valeur par défaut : True

Utiliser la base de données en tant que solution de secours pour la résolution du nom

Indique un recours à une adresse IP stockée dans une base de données MDB du gestionnaire ou une base de données du serveur lorsqu'un nom actif ne peut être résolu via les services de localisation d'adresse (DNS) ou NETBIOS.

Remarque : Dans la plupart des cas, l'option de solution de secours par défaut ne doit pas être modifiée et doit uniquement être modifiée sur demande du personnel de l'assistance technique de CA.

Les valeurs valides sont les suivantes :

1 = Tous les modes de secours sont activés

2 = Utiliser la solution de secours de la base de données du serveur

4 = Utiliser la solution de secours de la MDB

Valeur par défaut : 1

Utiliser les noms courts NETBIOS comme solution de secours

Indique si les noms courts NETBIOS sont utilisés comme solution de secours en cas d'échec de la recherche de nom complet (FQN).

Valeur par défaut : True

Remarque : Ces paramètres de configuration se trouvent dans le volet Stratégie de configuration/Stratégie par défaut de l'ordinateur/DSM/Composants communs/Réseau/Général. Pour plus d'informations, consultez la rubrique Groupe de stratégies Général (Réseau) dans la section Stratégie de configuration de l'*aide de l'explorateur DSM*.

- Si Client Automation est installé sur un ordinateur IPv4 seul et si IPv6 est activé ultérieurement, l'ordinateur doit être redémarré et le service CAF réinitialisé.
- Si votre réseau prend uniquement en charge IPv6 (c'est-à-dire, le routage IPv4 a été désactivé ou arrêté) ou utilise essentiellement les connexions IPv6, nous vous recommandons de modifier la valeur du paramètre de configuration "Définir la priorité des adresses résolues" sur ipv6, ipv4. Cette configuration améliorera les performances des communications entre les différents ordinateurs de l'entreprise ou du domaine.
- Si vous disposez d'un gestionnaire avec une MDB distante et un routage IPv6 uniquement entre le gestionnaire et la MDB distante, l'explorateur DSM s'ouvrira très lentement la première fois du fait que le paramètre de configuration "Définir la priorité des adresses résolues" est initialement défini sur ipv4, ipv6 par défaut. Dans ce cas, le nom reconnaît d'abord une adresse IPv4, puis l'adresse IPv6 est essayée, et réussie, après échec de la connexion à la base de données suite à l'expiration du délai. La stratégie de configuration peut uniquement être modifiée une fois l'explorateur DSM ouvert.

- Si votre réseau comporte un grand nombre d'ordinateurs Windows 2003 et Windows XP, le paramètre de configuration "Définir la priorité des recherches DNS" doit être laissé sur ipv4, ipv6, car les messages DNS sont uniquement envoyés par les connexions IPv4 sur ces plates-formes.

Résolution de noms DNS pour des ordinateurs hébergeant des composants DSM

Tous les ordinateurs hébergeant les composants DSM tels que le gestionnaire d'entreprise, le gestionnaire de domaines, le serveur de modularité et les agents, doivent prendre en charge la recherche DNS directe et inversée. Vérifiez que la communication entre les composants DSM fonctionne correctement.

Affectation d'un nom d'hôte à l'IP de bouclage

Client Automation requiert que le nom d'hôte puisse être résolu à tout moment aux fins de communications internes et externes. Le programme d'installation interactif contient l'option Assigned hostname to the loopback IP (Nom d'hôte affecté à l'IP de bouclage), qui tient compte de l'ancienne antérieure à définir.

Pour une installation autonome, dans la section Mise en réseau ou DNS du fichier autoinst.xml, définissez l'entrée write_hostname sur True comme suit :

```
<networking>
  <dns>
    <dhcp_hostname config:type="boolean" >false</dhcp_hostname>
    <dhcp_resolv config:type="boolean" >true</dhcp_resolv>
    <hostname>$HostName$</hostname>
    <write_hostname config:type=boolean>true</write_hostname>
  </dns>
</networking>
```

Vous trouverez le fichier autoinst.xml à l'emplacement suivant :

DSM_Install_Folder\server\SDBS\var\managedpc\images\IMAGE_NAME\IMAGE_NAME \suse

Prise en charge de la norme FIPS 140-2

La norme FIPS PUB 140-2 (Federal Information Processing Standard, Publication 140-2) est une norme de sécurité informatique adoptée par le gouvernement américain et qui prévoit l'accréditation des modules de chiffrement. Cette norme a été établie par le NIST (National Institute of Standards and Technology), qui se charge également de sa mise à jour.

Les produits informatiques dont le mode accrédité par la norme FIPS repose sur des modules de chiffrement bénéficiant de l'accréditation FIPS 140-2 peuvent uniquement utiliser les fonctions de sécurité approuvées FIPS comme AES (Advanced Encryption Standard) ou SHA-1 (Secure Hash Algorithm) et d'autres protocoles de niveau supérieur tels que TLS v1.0, conformément aux spécifications de la norme FIPS 140-2 et des manuels d'implémentation correspondants.

Dans Client Automation, le chiffrement traite les aspects suivants :

- Stockage et vérification des mots de passe
- Communication de toutes les données sensibles entre composants de produits CA, et entre produits CA et produits tiers

FIPS 140-2 spécifie les exigences liées à l'utilisation d'algorithmes de chiffrement dans des systèmes de sécurité de protection de données sensibles mais non classifiées.

Client Automation prend en charge les techniques de chiffrement conformes à la norme FIPS. Client Automation utilise les bibliothèques de chiffrement RSA BSafe et Crypto-C ME v2.1, dont le contenu a été validé comme étant conforme aux exigences de sécurité applicables aux modules de chiffrement déterminées par la norme FIPS 140-2.

Prise en charge de la plate-forme FIPS 140-2

Pour être conforme à la norme FIPS 140-2, l'utilisation d'un module cryptographique certifié FIPS 140-2 est requise en mode et configuration certifiés. Le module cryptographique RSA certifié n'est pas disponible pour toutes les plates-formes disposant de Client Automation. Pour les plates-formes ne disposant pas de module certifié mais pour lesquelles la stratégie de domaines requiert uniquement une cryptographie FIPS 140-2, la prise en charge de la cryptographie sur ces plates-formes utilise uniquement des algorithmes et des fonctions approuvés par la norme FIPS ; ils seront toutefois fournis par un module cryptographique non approuvé (CA OpenSSL).

Les plates-formes suivantes sont conformes à la norme FIPS 140-2 lorsqu'elles fonctionnent en mode FIPS uniquement :

- Plates-formes Windows NT x86
- Linux
- Solaris SPARC/32

Actuellement, toutes les autres plates-formes ne sont pas conformes à la norme FIPS 140-2 bien que, lors de la configuration en mode FIPS uniquement, elles utiliseront uniquement des algorithmes et des fonctions approuvés FIPS, mais non avec un fournisseur de cryptographie certifié.

Modes FIPS pris en charge

Client Automation prend en charge la cryptographie conforme à la norme FIPS dans deux modes : Préférence FIPS et FIPS uniquement. Les deux modes sont applicables au stockage et à la vérification de mots de passe, et à la communication de toutes les données sensibles entre plusieurs composants de produits CA, et entre des produits CA et des produits tiers.

Mode Préférence FIPS

Il s'agit du mode qui permet la rétrocompatibilité vers les versions précédentes de Client Automation. Dans ce mode, les composants de la version Version 12.9 utilisent une-cryptographie conforme à la norme FIPS lors de la communication avec un autre composant de la version Version 12.9. Pourtant, lorsqu'ils communiquent avec les composants de versions précédentes, ils peuvent utiliser des fonctionnalités de sécurité qui ne sont pas conformes à la norme FIPS pour prendre en charge la rétrocompatibilité. Le mode Préférence FIPS est le mode par défaut des nouvelles installations et le *seul* mode pris en charge pour les mises à niveau.

Remarque : Une fois tous les composants DSM mis à niveau dans votre environnement, vous pouvez basculer en mode FIPS uniquement.

Mode FIPS uniquement

Il s'agit du mode qui utilise uniquement des techniques conformes à la norme FIPS pour la cryptographie. Utilisez cette option pour les *nouvelles* installations Client Automation. Ce mode n'est pas rétrocompatible avec les versions précédentes de Client Automation.

Remarque : Les composants ne peuvent pas utiliser la cryptographie héritée, une fois le mode FIPS uniquement activé. Vous pouvez revenir au mode Préférence FIPS, si nécessaire.

Prise en charge du basculement et remplacement du matériel

CA Client Automation prend en charge le basculement dans un environnement en cluster, ainsi que le remplacement du matériel de gestionnaire en cas de panne ou de mise à niveau matérielle.

Pour plus d'informations, consultez les sections :

- Prise en charge de basculement (page 88)
- Remplacement de matériel du gestionnaire (page 91)

Prise en charge de basculement

La prise en charge de basculement est disponible uniquement pour les environnements d'exploitation Windows et les bases de données Microsoft SQL Server.

Le basculement prend en charge l'installation des composants du gestionnaire sur deux ordinateurs distincts exécutant Microsoft Cluster. L'un des systèmes doit constituer le nœud actif qui exécute la fonctionnalité de gestionnaire et les autres systèmes représentent le système passif en veille, avec le logiciel de gestionnaire installé, mais non activé.

Installation sur un cluster

Client Automation ne dispose d'aucune fonctionnalité de détection des pannes du système. Il est donc impossible basculer automatiquement du noeud actif vers le noeud passif en cas de panne du système.

Client Automation peut être installé en deux modes : soit comme gestionnaire ITCM actif, soit comme gestionnaire ITCM passif. Les termes Actif et Passif font référence au gestionnaire DSM actif ou passif ; ils ne font pas référence au nœud de cluster (qui peut être actif ou passif).

Lors de l'installation de Client Automation dans un cluster, une instance du gestionnaire DSM sera installé comme gestionnaire ITCM actif et chacune des autres instances sera installée comme gestionnaire ITCM passif.

Pour installer un gestionnaire ITCM actif :

1. Sur le noeud actif du cluster, lancez le programme d'installation Client Automation, puis réalisez une installation personnalisée.
2. Sélectionnez les composants du gestionnaire et tous les autres composants devant faire partie de l'installation.
3. Dans la boîte de dialogue Configurer le gestionnaire, saisissez le nom du serveur de la base de données de gestion.

4. Cliquez sur le bouton Récupération.
5. Dans la boîte de dialogue qui s'affiche, sélectionnez les options Activer la prise en charge de la récupération et Actif.
6. Entrez le nom du cluster et l'emplacement du lecteur partagé.

   Remarque : Si vous souhaitez installer un gestionnaire de domaines DSM avec un Microsoft SQL Server local dans un environnement en clusters Microsoft, Client Automation doit être installé dans le groupe de clusters de Microsoft SQL Server à l'aide du nom virtuel du Microsoft SQL Server.
7. Continuez à procéder à l'installation jusqu'à atteindre la boîte de dialogue Choisir l'emplacement de destination où vous pouvez configurer le dossier Destination.

   Le dossier Destination doit se trouver sur le disque local de l'ordinateur et non sur le disque du cluster partagé.

   L'emplacement des données de configuration doit indiquer le disque partagé du cluster. Cela se fait automatiquement selon les informations saisies dans la boîte de dialogue "basculement". Cependant, il est possible de vérifier ces emplacements en cliquant sur le bouton Avancé. L'emplacement des composants partagés doit également être sur le disque local de l'ordinateur ; cet emplacement est configuré à l'aide du bouton Avancé.
8. Cliquez sur Suivant, puis continuez dans les différentes boîtes de dialogue d'installation jusqu'à ce que l'installation commence.

   L'installation d'un gestionnaire avec CSS sur un ordinateur avec clusters est légèrement différente de celle sur un ordinateur sans cluster et autonome. Généralement, l'installation de CCS est silencieuse. Cependant, sur un cluster, Client Automation appellera une installation interactive de CCS.

   Important : Ne modifiez aucune des informations de ces boîtes de dialogue, car Client Automation les a remplies avec les valeurs appropriées ; cliquez simplement sur Suivant dans les boîtes de dialogue jusqu'à ce que l'installation de CCS commence.

Pour installer un gestionnaire ITCM passif :

1. Avant de procéder à l'installation sur l'autre ordinateur (ou ordinateurs) dans le cluster, vérifiez la disponibilité des groupes de cluster et la fonctionnalité des ressources partagées. Sinon, faîtes de l'ordinateur le noeud actif dans le cluster.
2. Lancez le programme d'installation Client Automation de la façon habituelle, puis procédez à une installation personnalisée.
3. Sélectionnez les mêmes composants que ceux sélectionnés lors de l'installation du gestionnaire ITCM actif.
4. Dans la boîte de dialogue Configurer le gestionnaire, saisissez le nom du serveur de la base de données de gestion.

5. Cliquez sur le bouton Récupération.
6. Dans la boîte de dialogue qui s'affiche, sélectionnez les options Activer la prise en charge de la récupération et Passif.
7. Ensuite, le programme d'installation demande l'emplacement du fichier DSMRecovery.ini.

   Il se situe dans le répertoire de données de configuration Client Automation, qui se trouve sur le disque partagé du cluster. L'emplacement aura été défini pendant l'installation du gestionnaire ITCM actif.
8. Cliquez sur Suivant, continuez dans les différentes boîtes de dialogue d'installation, puis commencez l'installation.

   A l'instar de l'installation du gestionnaire ITCM actif, l'installation de CCS est réalisée de façon interactive.

   Important : Ne modifiez aucune des informations de ces boîtes de dialogue, car Client Automation les a remplies avec les valeurs appropriées ; cliquez simplement sur Suivant dans les boîtes de dialogue jusqu'à ce que l'installation de CCS commence.

Une fois les installations terminées, les ressources du cluster peuvent être remises dans le nœud actif du cluster.

Lorsque le noeud de cluster actif bascule entre les ordinateurs dans le cluster, le gestionnaire ITCM passif doit être averti. Vous avertissez le gestionnaire en exécutant le fichier ActivateManagerNode.bat, qui se trouve dans le répertoire bin à l'emplacement de l'installation du gestionnaire DSM. Sinon, si un système de gestion des clusters doit être utilisé, le gestionnaire de cluster peut être configuré pour exécuter le contenu du fichier .bat.

Remarques :

- Pour plus d'informations sur la configuration de clusters, consultez le livre vert intitulé Client Automation/CA Unicenter Desktop & Server Management à l'adresse http://ca.com/greenbooks.
- En cas d'installation sur une instance SQL nommée non par défaut, assurez-vous que les numéros de ports TCP/IP de l'instance sont identiques sur tous les nœuds du cluster. Si tel n'est pas le cas, modifiez les numéros de port en conséquence. Assurez-vous également que le navigateur de SQL Server est actif.
- Actuellement, aucun serveur amorçable n'est pris en charge sur un cluster.

- Sous Windows 2008 (et Windows Vista) le fichier de commandes ActivateManagerNode.bat doit être exécuté avec des droits d'administrateur complets. Si vous êtes connecté en tant qu'administrateur, par défaut cet utilisateur possède automatiquement des droits complets. Toutefois, si vous êtes connecté en tant qu'autre utilisateur appartenant également au groupe Administrateurs, Windows s'organise de telle façon à ce que cet utilisateur dispose uniquement de droits ordinaires et, par conséquent, ne puisse pas exécuter ce fichier de commandes correctement. Pour éviter ce problème, le fichier de commandes ActivateManagerNode.bat doit être exécuté par un utilisateur avec élévation de privilèges. Par exemple, pour ouvrir une fenêtre de ligne de commande avec élévation de privilèges, cliquez avec le bouton droit de la souris sur l'icône Invite de commande et sélectionnez Exécuter en tant qu'administrateur. Vous pouvez donc exécuter le fichier de commandes à partir d'ici.

Remplacement de matériel du gestionnaire

Il est possible de remplacer le matériel du système de gestionnaire en cas de panne du système ou de mise à niveau matérielle, car la MDB et les paramètres de configuration d'origine peuvent être utilisés.

Il est inutile de réinstaller la MDB ou de reconfigurer la bibliothèque Software Delivery ou les carnets d'adresses Remote Control, car la configuration d'origine peut être utilisée.

Pour se préparer à l'éventualité d'un remplacement du système de gestionnaire, vous devez paramétrer quelques éléments dans l'assistant d'installation. Dans la boîte de dialogue Configurez un gestionnaire se trouve un bouton appelé Récupération qui permet d'accéder à la boîte de dialogue de basculement. Dans la boîte de dialogue de basculement, vous devez sélectionner les options Remplacement du système et Activer le remplacement. Dans la boîte de dialogue concernant les répertoires d'installation, définissez les répertoires pour les données du gestionnaire (données MDB et de configuration) à l'aide d'un chemin qui doit être régulièrement sauvegardé. Au cours de l'installation, toutes les entrées fournies via les différentes boîtes de dialogue sont stockées dans un fichier nommé DSMRecovery.ini, puis sont enregistrées à l'emplacement des données de configuration spécifié. A l'aide de ce fichier, vous pouvez remplacer le matériel en cas de panne.

Si le matériel a été remplacé et que le gestionnaire doit être réinstallé, exécutez à nouveau la boîte de dialogue Récupération, sélectionnez Activer le remplacement, ainsi que l'option Remplacement du système.

Au bas de la boîte de dialogue, saisissez le chemin d'installation des données de configuration afin que le programme d'installation trouve le fichier stocké DSMRecovery.ini. Le programme d'installation lit tous les paramètres d'installation et utilise les mêmes MDB, bibliothèque logiciel, etc. que celles de l'installation originale du gestionnaire.

Le chemin relatif vers les données de configuration doit être identique à celui du gestionnaire actif.

Le remplacement du système de gestionnaire exige que l'ancien et le nouveau matériel du gestionnaire utilisent un nom de système identique.

Remarque : en cas de panne matérielle d'ordinateur, aucune cohérence entre les données ne peut être assurée.

Configuration de CA HIPS en vue de l'installation de Client Automation

Si vous installez Client Automation sur un ordinateur où est installé un client CA HIPS (Host-Based Intrusion Prevention System), vous devez configurer le serveur CA HIPS avant d'installer Client Automation sur le poste client.

Pour configurer CA HIPS en vue de l'installation de Client Automation :

1. Sur l'ordinateur serveur CA HIPS, ouvrez une session sur la console CA HIPS.
2. Cliquez sur Gestion des stratégies, Définitions, Référentiel d'applications.
3. Si la liste des groupes ne contient pas de groupe SafeApps, créez-le et procédez comme suit :
    a. Cliquez sur Gestion des stratégies, Définitions, Paramètres courants, Paramètres globaux de sécurité du SE.
    b. Sélectionnez SafeApps dans la liste déroulante Groupe d'applications devant contourner les hooks en mode utilisateur et cliquez sur OK.
    c. Cliquez sur Gestion des stratégies, Définitions, Référentiel d'applications.
4. Sélectionnez le groupe SafeApps.
5. Cliquez sur Nouveau et entrez les détails suivants pour définir le fichier setup.exe :

Champ	Valeur
Type de membre	Application
Nom de membre	setup.exe
Identifié par	FileName

Champ	Valeur
Chemin	setup.exe
Groupes	SafeApps

6. Cliquez sur OK.
7. Cliquez sur Nouveau et entrez les détails suivants pour définir le fichier CACMS.MSI :

Champ	Valeur
Type de membre	Application
Nom de membre	CACMS.MSI
Identifié par	FileName
Chemin	CACMS.MSI
Groupes	SafeApps

8. Cliquez sur OK.
9. Cliquez sur Gestion des stratégies, Déploiement.
10. Cliquez sur Déployer.
11. Indiquez le numéro de version et cliquez sur OK.
12. Attendez que la stratégie soit activée sur le poste client CA HIPS.

    Le poste client CA HIPS est maintenant prêt pour l'installation de Client Automation.

Remarques relatives aux composants de l'infrastructure

La relation entre les divers composants de Client Automation est la suivante :

- Les agents ont une relation plusieurs-à-un avec leur serveur de modularité. Chaque agent rend compte à un seul serveur de modularité.
- Les serveurs de modularité ont une relation plusieurs-à-un avec leur gestionnaire de domaine. Chaque serveur de modularité doit rendre compte à un seul gestionnaire de domaine.
- Les gestionnaires de domaine ont une relation plusieurs-à-un facultative avec un gestionnaire d'entreprise. Chaque gestionnaire de domaine peut rendre compte à un seul gestionnaire d'entreprise.

Etapes d'installation d'infrastructure

Une installation d'infrastructure réussie est obtenue via la méthodologie de haut niveau suivante :

- Détermination de l'emplacement approprié des composants

  Cette étape consiste à décider quels ordinateurs jouent quel rôle, en fonction de considérations telles que la bande passante réseau, la charge système existante et d'autres aspects.

- Vérification de la configuration de votre réseau

  La configuration DNS doit permettre d'effectuer une recherche de type "nslookup *IP_address*" dans les connexions verticales de la hiérarchie multiniveau Client Automation (gestionnaire d'entreprise–gestionnaire de domaines, gestionnaire de domaines–serveur de modularité, serveur de modularité–agent, gestionnaire de domaines–agent).

- Installation des gestionnaires d'entreprise et de domaine
- Installation de serveurs de modularité
- Installation d'agents
- Installation des consoles administratives de l'explorateur DSM

Facteurs de dimensionnement d'infrastructure

Un certain nombre de facteurs ont un impact considérable sur le dimensionnement de l'infrastructure et sur les performances du système.

Charge sur les tâches de gestion des actifs

La taille de l'infrastructure est affectée par la charge des tâches Asset Management suivantes :

- Nombre d'attributs d'inventaire collectés
- Fréquence de la collecte d'inventaire

Charge sur les tâches de distribution de logiciels

La taille de l'infrastructure est affectée par la charge des tâches Software Delivery suivantes :

- Taille des packages logiciels à distribuer
- Quantité de packages logiciels à distribuer
- Gestion de la bande passante réseau
- Fréquence de livraison des packages logiciels (quotidienne, hebdomadaire, mensuelle, etc.)

Identification des ordinateurs dans Client Automation

Client Automation affecte un identifiant unique universel (UUID) propre à CA Technologies à chaque ordinateur géré. Ces données sont stockées sur chaque ordinateur aux emplacements suivants :

registre Windows :

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\HostUUID
```

Linux/UNIX :

```
/etc/cadmuuid
```

Le cadre d'applications (CAF) de CA ITCM recherche régulièrement un UUID spécifique de CA Technologies à ces emplacements. Si UUID est trouvé, le CAF considère qu'il s'agit d'un actif déjà enregistré dans la base de données. Si aucun UUID n'est trouvé, le CAF en crée un et enregistre l'actif dans la base de données.

Si vous avez copié une installation (vidage physique du disque dur à l'aide d'un outil de création d'image tel que GHOST ou fichier image d'un ordinateur virtuel en utilisant un outil tel que VMWare) pour l'installer sur un autre ordinateur, ou seulement à des fins de sauvegarde, l'installation copiée contient un UUID spécifique de CA de l'ordinateur d'origine. Si vous lancez cette installation copiée sur un ordinateur différent de celui d'origine, cet UUID propre à CA apparaîtra en double.

Pour empêcher la duplication d'UUID propres à CA, Client Automation effectue les actions suivantes :

1. Lorsque le CAF démarre ou lorsque la commande caf register est envoyée, un algorithme est exécuté pour vérifier si l'ordinateur cible est l'ordinateur d'origine ou un autre ordinateur.
2. Si l'ordinateur cible est l'ordinateur d'origine, l'UUID propre à CA d'origine est utilisé. Dans le cas contraire, un UUID propre à CA est créé.

Pour déterminer si un UUID spécifique de CA unique est requis, CA ITCM peut utiliser l'algorithme par défaut (recommandé) ou l'algorithme hérité. L'algorithme compare les caractéristiques suivantes de l'ordinateur cible aux valeurs dans la base de données :

Ordinateur virtuel

L'ID du système (attribut BIOS de système) est la seule caractéristique vérifiée par l'algorithme.

Ordinateur physique

- Conformité des adresses MAC

  Ce critère est rempli lorsqu'une des adresses MAC correspond à une des adresses MAC d'origine de la cible.

- Conformité des numéros de série de disque dur

  Ce critère est rempli lorsqu'un des numéros de série de disque dur correspond à un des numéros de série de disque dur originaux de la cible.

- Conformité de l'ID du système

  Ce critère est rempli lorsque l'ID du système correspond à l'ID du système d'origine de la cible.

Le changement des valeurs des caractéristiques précédentes n'implique pas nécessairement le changement de l'UUID spécifique de CA. Les remarques suivantes concernent l'application d'un changement de l'UUID spécifique de CA par l'algorithme :

- Un changement de valeur se produit uniquement si la valeur d'origine de la caractéristique existe dans la base de données et si la nouvelle valeur est différente de la valeur d'origine.

  Par exemple, si l'ancienne liste d'adresses MAC n'est pas disponible dans la base de données pour la comparaison, la modification d'un UUID spécifique de CA *ne sera pas* appliquée.

- Un changement de valeur se produit uniquement si les nouvelles valeurs d'adresses MAC ou les numéros de série de disque correspondent aux valeurs existantes dans la base de données.

Verrouillage de l'UUID d'hôte

En général, un changement de matériel entraîne un changement de l'UUID d'hôte. Si vous ne souhaitez pas le modifier, vous pouvez le verrouiller.

- Pour verrouiller l'hôte sous Windows, créez une valeur de chaîne LegacyHostUUID avec pour valeur 1, sous la clé de registre HKLM\Software\ComputerAssociates\HostUUID.
- Pour verrouiller l'UUID d'hôte sous Linux ou UNIX, créez un fichier nommé /etc/calockuuid.

Algorithme par défaut (Recommandé)

L'algorithme par défaut détecte les disques IDE et SCSI et détermine précisément le changement dans l'hôte en comparaison avec l'algorithme hérité, qui ne détecte que les disques IDE.

Une fois les caractéristiques de l'ordinateur cible vérifiées par l'algorithme, un UUID CA est généré dans les cas suivants :

- Les numéros de série du disque dur, ainsi que les adresses MAC ou l'ID système, ont été modifiés.
- Les numéros de série du disque dur ne sont pas détectés ; les ID système et les adresses MAC ont été modifiés.

Remarque : Pour un ordinateur virtuel, un changement de l'ID système entraîne un nouvel UUID d'hôte.

Algorithme hérité

Vous pouvez activer l'algorithme hérité aux fins d'identification des ordinateurs dans Client Automation.

Important : Activez l'algorithme hérité avant de mettre à niveau ou de lancer une nouvelle installation. Si vous passez en algorithme hérité après la mise à niveau ou l'installation, l'UUID CA généré sera incorrect.

Pour activer l'algorithme hérité, utilisez l'une des méthodes suivantes sous Windows, Linux, ou UNIX :

- Sous Windows, créez une valeur de chaîne LegacyHostUUID avec pour valeur 1, sous la clé de registre HKLM\Software\ComputerAssociates\HostUUID.
- Sous Linux ou UNIX, créez un fichier nommé /etc/calegacyuuid.

Remarque : Vous devez activer l'algorithme hérité sur tous les ordinateurs exécutant un agent CA ITCM.

Pour un ordinateur physique, l'algorithme vérifie les trois caractéristiques décrites plus haut. Si au moins deux critères sur trois ne sont pas satisfaits, le système cible sera considéré comme un nouvel ordinateur et un nouvel UUID CA sera créé.

Important : Les UUID générés par des versions antérieures du logiciel de gestion de poste de travail CA Technologies, tels qu'Unicenter® Software Delivery, Unicenter® Asset Management, et Unicenter® Remote Control, risquent de ne pas être uniques.

Ordinateurs itinérants entre domaines

Un ordinateur peut rendre compte à plusieurs gestionnaires de domaines différents. Cette fonctionnalité permet d'éviter les entrées dupliquées dans le gestionnaire d'entreprise lorsqu'un ordinateur se déplace entre des domaines liés au même gestionnaire d'entreprise.

Les informations (logiciels distribués, attributs d'inventaire, etc.) des ordinateurs membres d'un domaine différent sont déplacées vers le nouveau gestionnaire de domaines.

L'ordinateur est supprimé du domaine dont il vient. Par défaut, cette tâche est effectuée par la fonctionnalité de livraison de logiciels (si elle est installée). Si la fonctionnalité de distribution de logiciels n'est pas installée ou qu'elle est configurée pour ne pas conserver l'historique des jobs, la suppression de l'ordinateur est effectuée par le job de réplication.

Exemple : ordinateur itinérant

Les gestionnaires de domaines A et B sont liés au même gestionnaire d'entreprise. Un ordinateur X s'enregistre auprès du gestionnaire de domaines A et est répliqué dans le gestionnaire d'entreprise. L'ordinateur X s'enregistre ensuite auprès du gestionnaire de domaines B.

Avant que le gestionnaire de domaine B ne réplique l'ordinateur X dans le gestionnaire d'entreprise, il détermine si un ordinateur possédant le même UUID (c'est-à-dire un UUID ou hostuuid propre à CA Technologies) existe déjà dans l'entreprise. Il détecte l'ordinateur X du domaine A et sait à présent que cet ordinateur X s'est déplacé du gestionnaire de domaine A vers le gestionnaire de domaine B. Le compte "domaine A/ordinateurX" est supprimé sur le gestionnaire d'entreprise par la réplication du gestionnaire de domaine B et une notification d'itinérance est stockée dans la base de données du gestionnaire d'entreprise. Le compte "domaine B/ordinateur X" est répliqué dans le gestionnaire d'entreprise. Avant que le gestionnaire de domaine A ne réplique les modifications ou les nouveaux ordinateurs, il détermine s'il existe des notifications d'itinérance. Il trouvera alors la notification pour l'ordinateur X et la supprimera sur le gestionnaire de domaine A. (Si un agent Software Delivery est installé sur l'ordinateur itinérant, il n'est pas supprimé immédiatement.)

L'ordinateur X a maintenant été déplacé avec succès et existe dorénavant uniquement comme compte "domaine B/ordinateur X" dans l'environnement du gestionnaire d'entreprise.

Déconnexion personnalisable ou bannière de redémarrage

Lorsque les fonctions Software Delivery ou Remote Control initient une déconnexion ou un redémarrage de l'ordinateur cible, le cadre d'applications communes (CAF) affiche une boîte de dialogue avec une bannière bitmap et informe l'utilisateur de ce qui se passe.

Vous pouvez remplacer le bitmap de bannière par défaut par votre propre bannière, en créant un fichier d'image bitmap (avec l'extension de fichier .bmp) d'une taille de 500 x 65 pixels. Stockez ce fichier sur un disque local ou un partage réseau puis définissez la stratégie de configuration Composants communs/CAF/Général/Boîte de dialogue CAF : nom du fichier bitmap sur le nom de chemin du fichier. Lorsque la boîte de dialogue s'affiche, elle lit ce fichier et affiche l'image.

Utilisation d'un programme de redémarrage

Le CAF transmet généralement les demandes de redémarrage du système vers le système d'exploitation afin d'effectuer le redémarrage réel. Vous pouvez utiliser un programme de redémarrage personnalisé, capable de tenir compte de certaines exigences.

Pour activer et configurer l'utilisation d'un programme de redémarrage du système personnalisé, les paramètres de stratégie de configuration suivants sont disponibles dans ...DSM/commun/groupe de stratégies de configuration générales :

CAF : commande de redémarrage

Spécifie le nom du programme de redémarrage personnalisé à utiliser au lieu de l'API du système d'exploitation. Si aucun programme de redémarrage n'est spécifié, l'API du système d'exploitation est utilisée.

Boîte de dialogue du CAF : activer la boîte de dialogue

Spécifie si une boîte de dialogue de compte à rebours s'affiche (valeur = True) ou si un redémarrage immédiat sans boîte de dialogue de compte à rebours est effectué (valeur = False). Cela s'avère avec sur du matériel spécialisé, qui risque de n'autoriser aucune interaction entre l'utilisateur et une boîte de dialogue.

Boîte de dialogue de redémarrage et de déconnexion sur les serveurs de terminaux

Lors du redémarrage, une boîte de dialogue vous indiquant ce qu'il se passe et à quel moment s'affiche. Elle présente plusieurs boutons qui permettent un certain contrôle du processus.

Redémarrer maintenant

Lance le redémarrage maintenant plutôt que d'attendre le délai indiqué.

Différer

Diffère le redémarrage pendant quelques instants, afin de vous laisser le temps de terminer ou de sauvegarder votre travail.

Annuler

Abandonne le redémarrage.

Ce bouton fonctionne correctement sur un ordinateur dont vous êtes le seul utilisateur car personne d'autre n'est affecté. Cependant, le fonctionnement de ce bouton est différent sur un serveur de terminaux, qui peut être utilisé par plusieurs utilisateurs. Tous les boutons sont en effet désactivés, car l'activation de l'un d'entre eux peut affecter tous les autres utilisateurs sans qu'ils ne soient au courant ni même consentants. De plus, puisque l'ordinateur est "détenu" par l'administrateur système, ce dernier est le seul à posséder les droits nécessaires au contrôle du processus de redémarrage.

Lors d'une déconnexion, le bouton Déconnecter maintenant est néanmoins activé étant donné qu'il n'affecte que vous. Les boutons Différer et Annuler sont là encore désactivés.

Emplacement de la documentation des services Web et du fichier WSDL

Le *manuel de référence des services Web* est disponible aux emplacements suivants :

- Système de documentation CA Client Automation principal
- Aux emplacements suivants si les services Web sont installés :

  http://%*nom_machine*%/UDSM_R11_WebService/help/index.htm (sous Windows)

  http://%*nom_machine*%/UDSM_R11_WebService/help (sous Linux)

Si les services Web ont été installés, le *fichier WSDL* se trouve aux emplacements suivants sous Windows :

- http://%*nom_ordinateur*%/UDSM_R11_WebService/wsdl

%*votre_répertoire_installation*%\CA\DSM\webservices\wsdl

Sous Linux, le *fichier WSDL* se trouve à l'emplacement suivant :

- %*votre_répertoire_installation*%/CA/DSM/webservices/wsdl

Eléments à prendre en compte pour la console Web et les services Web

Voici les éléments à prendre en compte pour l'installation et l'intégration de la console Web et des services Web.

Installation des packages requis pour la console Web

Le tableau ci-dessous répertorie les packages tiers et CA Technologies prérequis pour la console Web :

Package	Système d'exploitation	Description/Commentaire
AMS	Windows et Linux	Composant CA Technologies pour le système de maintenance des actifs AMS est utilisé par la console Web pour afficher des informations relatives aux actifs détenus et détectés.
Serveur Web Apache	Linux	Composant d'hébergement de l'application de la console Web Si vous souhaitez utiliser une version spécifique du serveur Web Apache, vous devez configurer la variable CA_DSM_USE_APACHE_PROG sur le chemin complet du binaire plutôt que sur son répertoire parent avant de démarrer l'installation de CA Client Automation. Par exemple : CA_DSM_USE_APACHE_PROG=/apache2.2.8/bin/httpd

Package	Système d'exploitation	Description/Commentaire
AMS	Windows et Linux	Composant CA Technologies pour le système de maintenance des actifs AMS est utilisé par la console Web pour afficher des informations relatives aux actifs détenus et détectés.
Apache Tomcat	Windows et Linux	Conteneur de servlets pour la console Web
Connecteur Apache Tomcat pour ISAPI	Windows	Connecteur entre Internet Information Services (IIS) et Tomcat
Connecteur Apache Tomcat pour Apache (mod_jk)	Linux (32 et 64 bits)	Connecteur entre serveur Web Apache et Tomcat
Pilote JDBC d'Oracle	Windows et Linux	Pilote JDBC utilisé pour la connexion à une base de données Oracle
Apache Axis	Windows et Linux	Boîte à outils Service Web
CA CMDB	Windows et Linux	Base de données de gestion de la configuration
CA Service Desk	Windows et Linux	
Microsoft IIS	Windows	Composant Microsoft Internet Information Services qui héberge l'application de console Web.
Log4j	Windows et Linux	Boîte à outils de connexion
Pilote JDBC Microsoft SQL Server	Windows	Pilote JDBC utilisé pour se connecter à une base de données SQL Server.
Pilote JDBC Microsoft SQL Server	Linux	Pilote JDBC utilisé pour se connecter à une base de données SQL Server.
Sun JRE	Windows et Linux	Environnement d'exécution Sun Java Requis pour la console Web avec IPv6.

Important : La modification de la clé SQLServer.PortNo avec le numéro de port de base de données dans le fichier wacconfig.properties n'est plus prise en charge. Vous devez fournir le numéro de port correct pendant l'installation, car il ne peut pas être modifié ultérieurement.

Installation de la console d'administration Web ou des services Web sur des ordinateurs Linux 64 bits

Client Automation ne prend pas en charge les serveurs Web Apache 64 bits sur les ordinateurs Linux. Désinstallez les serveurs Web Apache 64 bits avant d'installer la console Web Client Automation ou les services Web Client Automation sur un ordinateur Linux 64 bits.

Utilisation de port Tomcat par la console Web

La console Web utilise le moteur de servlet web Apache Tomcat. Par défaut, les numéros de ports de Tomcat sont 8090 (démarrage), 8095 (arrêt) et 8020 (AJP).

L'écran des ports Tomcat est rempli au cours de l'installation. L'utilisateur doit fournir le numéro de port correct pendant l'installation.

Le port de Tomcat utilisé par la console Web se trouve dans le fichier server.xml, sous le chemin d'installation du système.

Sous Windows, l'emplacement du fichier server.xml est le suivant :

`[`*`chemin_installation`*`]\Web Console\conf\server.xml`

Sous Linux, l'emplacement du fichier server.xml est le suivant :
`[`*`chemin_installation`*`]/webconsole/conf/server.xml`

Configuration de port Tomcat pour la console Web

Il peut arriver qu'un ou tous les ports par défaut de Tomcat soient déjà utilisés par d'autres applications CA Technologies déjà installées sur l'ordinateur. Le programme d'installation de la console Web vérifie quels sont les ports déjà utilisés et affecte automatiquement de nouveaux numéros de ports en conséquence.

Les applications utilisant les numéros de port en conflit doivent fonctionner au moment de l'installation pour permettre leur détection. Si ce n'est pas le cas, il est nécessaire d'exécuter une procédure manuelle après l'installation pour résoudre les conflits de numéros de ports. Lorsque différentes applications tentent d'utiliser les mêmes numéros de port, leur démarrage peut échouer. Généralement la première application qui essaye de démarrer y arrive, et celles qui essaient ensuite échouent.

Pour modifier les numéros de port que la console Web utilise

1. Arrêtez l'instance de console Web de Tomcat, s'il est en cours d'exécution, en ouvrant une console de commandes et en tapant :
   ```
   caf stop tomcat
   ```
2. Ouvrez le fichier server.xml file dans un éditeur de texte.

   Ce fichier contient normalement des entrées ressemblant à ce qui suit :

   ```
   <Server port="8095" shutdown="SHUTDOWN" debug="0">
   ```

   ```
   <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
       port="8090" minProcessors="5" maxProcessors="75"
       enableLookups="true" redirectPort="8443"
       acceptCount="100" debug="0" connectionTimeout="20000"
       useURIValidationHack="false" disableUploadTimeout="true" />
   ```
3. Remplacez les numéros de port *nnnn* dans les affectations port="*nnnn*" (il en existe 2 dans l'exemple ci-dessus) par des ports libres disponibles.
4. Enregistrez le fichier et quittez l'éditeur de texte.
5. Démarrez l'instance de console Web de Tomcat en ouvrant une console de commandes et en tapant :
   ```
   caf start tomcat
   ```

Si vous n'êtes pas certains des numéros de port pouvant être utilisés par d'autre applications, essayez d'incrémenter tous les numéros de port de 1. Démarrez ensuite les applications, et si vous rencontrez encore des problèmes, répétez le processus décrit ci-dessus.

Déploiement d'une console Web autonome

Vous pouvez déployer une console Web, soit sur l'ordinateur du gestionnaire DSM soit sur un autre ordinateur. Pour obtenir une performance optimale, nous recommandons que l'ordinateur hébergeant la console Web autonome et l'ordinateur hébergeant la MDB et le gestionnaire de domaines soient situés dans le même sous-réseau (au même emplacement géographique).

Console Web : Visionneuse CMDB

La visionneuse CMDB (Configuration base de données de gestion) est une interface utilisateur basée sur le Web qui affiche la relation entre les différents éléments de configuration au sein de la base de données CMDB. Deux conditions préalables sont que la CMDB doit être installée sur la même MDB que le gestionnaire de domaine et que la stratégie de configuration d'intégration de Service Desk doit être appliquée sur l'ordinateur où la Console d'administration Web (CAW) est installé.

La visionneuse CMDB peut être lancée depuis la section Lancement rapide de la page d'accueil, comme suit :
ordinateur`/Homepage/Quick Launch/External Applications/CMDB Visualizer`

La visionneuse CMDB doit être installée séparément et n'est pas inclue dans l'installation Client Automation.

Dépendances internes

Certains composants DSM présentent des dépendances internes par rapport à d'autres composants DSM. Au cours de l'installation, les composants sélectionnés sont examinés afin de détecter les dépendances internes. S'ils dépendent d'autres composants DSM, ces composants sont automatiquement installés.

Par exemple, dans le cadre de la fonction Software Delivery (SD), la fonction du serveur de modularité nécessite la présence d'un agent SD sur le même système. Par conséquent, même si les agents n'ont pas été sélectionnés pour l'installation, l'agent SD est automatiquement installé si le serveur de modularité a été sélectionné pour l'installation.

Voici les dépendances qui entraînent l'installation automatisée de composants DSM supplémentaires :

Gestionnaire :

Composant	Nécessite ...
Gestionnaire (SD)	Tous les composants DTS (gestionnaire et agent) sur le même système. Serveur de modularité, s'il s'agit d'un gestionnaire de domaines.

Composant	Nécessite ...
Gestionnaire (d'entreprise ou de domaines)	Module d'extension du gestionnaire Asset Management. Moteur
Gestionnaire d'entreprise	Agent DTS
Console Web	Services Web

Serveur :

Composant	Nécessite ...
Serveur de modularité (SD)	Agent SD sur le même système Agent DTS

Agent :

Composant	Nécessite ...
Catalogue (SD)	Agent SD sur le même système

Dépendances par rapport à d'autres produits sous Windows

Certains packages d'installation MSI présentent des dépendances par rapport à d'autres produits tiers. Certains sont installés automatiquement par l'installeur Client Automation, tandis que d'autres doivent être commandés et installés par le client.

Package d'installation Client Automation	Prérequis tiers	Partie de l'image d'installation ?	Installation de configuration maître ? (*)
Explorer – module d'extension Reporter	Client DB	Non	Non
Gestionnaire – tous les modules d'extension	Pour MDB – Client DB ou serveur DB local	Non	Non

Package d'installation Client Automation	Prérequis tiers	Partie de l'image d'installation ?	Installation de configuration maître ? (*)
Gestionnaire – module d'extension Asset Management	SUN Microsystems J2SE JRE (Java Runtime Environment, environnement d'exécution Java)	Oui	Oui - JRE fait partie de l'installation du gestionnaire et est automatiquement installé au cours d'une installation personnalisée ou via l'installation du gestionnaire à l'aide de la ligne de commande MSI
services Web	Microsoft Internet Information Server (IIS) 7.0 **Remarque :** L'installation par défaut d'IIS que 7.0 n'installe pas la console Web requise pour les composants, mais installe les extensions et filtres ISAPI, avant que vous installiez la console Web.	Non	Non

Package d'installation Client Automation	Prérequis tiers	Partie de l'image d'installation ?	Installation de configuration maître ? (*)
Console Web	Apache Jakarta Tomcat 5.5.12	Oui	Oui - Tomcat fait partie de l'installation du gestionnaire et est automatiquement installé au cours d'une installation personnalisée ou via l'installation du gestionnaire à l'aide de la ligne de commande MSI
	Oracle J2SE JRE 1.7.0_17 Java Runtime Environment (JRE)	Oui	Oui - JRE fait partie de l'installation du gestionnaire et est automatiquement installé au cours d'une installation personnalisée ou via l'installation du gestionnaire à l'aide de la ligne de commande MSI
	AMS 1.6.2	Oui	Oui, uniquement au cours d'une installation personnalisée

(*) Certains packages marqués Oui pour l'installation automatisée sont installés uniquement lors de l'utilisation de l'assistant d'installation interactive. Ils ne sont pas installés par appel direct du package MSI. Ce comportement dépend de la technologie et du format utilisés pour ces packages fournis à l'installeur Client Automation.

Par conséquent, lors de la distribution de composants du gestionnaire à d'autres systèmes à l'aide des fonctions Software Delivery ou de l'assistant de déploiement, certains prérequis doivent d'abord être installés manuellement avant l'installation du package de composants.

Installation des éléments prérequis manuellement sous Windows

Quelques exemples de commande et de procédures sont présentés ci-dessous afin de vous aider à installer les éléments prérequis pour les packages d'installation.

- **Installation de CA Asset Maintenance Sytem (AMS) :**

  ```
  WindowsProductFiles_x86\AMS\setupwin32console.exe -P
  installLocation="c:\Program Files\CA\DSM\Web Console\webapps\AMS" -V
  SERVERNAME="nom_système_gestionnaire" -V WEBPORT="port_démarrage_Tomcat" -V
  DASSERVERNAME="nom_serveur_MDB" -V INGRESLISTENER="nom_instance_BdD" -silent
  ```

- **Installation de MSAARDK :**

  ```
  WindowsProductFiles_x86\MSAARDK\MSAARDK.exe /R:N
  ```

S'il est nécessaire d'installer un élément à partir de la ligne de commande ou d'un fichier de commandes, nous vous suggérons l'approche suivante. Pour déterminer les éléments à installer et les lignes de commande à exécuter, procédez à une installation modèle pour la combinaison particulière de fonctionnalités du gestionnaire. L'installeur crée plusieurs fichiers journaux sous le répertoire %temp%. La commande peut être trouvée via l'ouverture du fichier DSMSetup.log et la recherche de Launch ciCCSSetup. Vous accédez ainsi à la section des commandes exécutées pour installer les différents composants.

D'autres recherches de Launch peuvent être effectuées, ce qui vous permet de déterminer les commandes msiexec pour l'installation des éléments suivants :

- AMS
- Agents
- Serveur de modularité
- explorateur DSM
- Gestionnaire
- etc.

Chaque ligne de commande affiche les propriétés à utiliser lors de l'appel de la commande et peut être copiée dans le script d'automatisation. Tous les paramètres importants sont expliqués dans la section Outil d'installation msiexec. (page 181)

Dans le cas d'une installation par le gestionnaire, la MDB doit être installée et configurée comme premier package avant l'installation de tout autre élément.

Dépendances par rapport à d'autres produits sous Linux et UNIX

Dans les versions Linux et UNIX de CA Client Automation, des composants tiers tels que Java Runtime Environment sont intégrés dans les images DVD sous forme de packages PIF ou RPM, et sont installés en fonction des besoins lors de l'installation d'un package DSM. Aucune procédure d'installation manuelle n'est généralement requise.

Cependant, sur certaines versions de Linux, les bibliothèques de compatibilité d'exécution doivent être installées avant l'installation des composants DSM. Pour plus d'informations, reportez-vous à la section Bibliothèques de compatibilité pour Linux.

Sous Linux, la barre d'état système nécessite l'installation de GIMP Toolkit GTK+ 1.2 (version exacte). Le GTK n'est pas fourni avec CA Client Automation ; vous devez télécharger la version requise à l'adresse www.gtk.org.

Un contrôle complet de la sélection des packages est disponible au cours de l'installation de Linux et UNIX avec des paramètres de fichier de réponses, conjointement avec l'option de ligne de commande /R pour la commande installation. Les options disponibles sont décrites sous Installation de Client Automation via la ligne de commande sous Linux et UNIX (page 202).

Redémarrage d'Apache sous Linux

Si vous devez redémarrer Apache, ne le faites pas à l'aide de l'IUG car celle-ci ne sélectionne pas l'environnement requis par CA Client Automation. A la place, vous pouvez par exemple accéder à un shell et démarrer Apache depuis ce dernier utilisant la commande :

```
dsm_restart_apache [-f]
```

L'option -f démarre Apache s'il n'est pas en cours d'exécution.

Si vous ne spécifiez pas l'option -f et si Apache n'est pas en cours d'exécution, il ne sera pas démarré. Si Apache est déjà en cours d'exécution, il sera redémarré.

Chapitre 3: Installation de Client Automation

Le chapitre suivant comporte des informations sur le processus général et les exigences de l'installation de Client Automation. Vous pouvez ignorer certaines sections au début du chapitre qui comportent des informations et des remarques d'installation très spécifiques aux composants DSM et lire directement l'introduction au programme d'installation et au processus d'installation. Ci-après, les descriptions de l'installation interactive et de l'installation à l'aide de la ligne de commande.

Ce chapitre traite des sujets suivants :

Compréhension du processus d'installation

Le processus d'installation comprend trois étapes principales :

1. Phase de préparation
2. Phase interactive
3. Phase d'exécution

Au cours de la phase de préparation, vous examinez les options du produit et rassemblez toutes les informations nécessaires à l'installation, comme indiqué dans les premières sections de ce chapitre. Vous devrez ensuite vérifier les prérequis logiciels existants ou les installer, puis sélectionner et démarrer l'installation de toute fonction du produit fournie avec le support d'installation.

Au cours de la phase interactive, vous fournissez les informations rassemblées à l'étape 1 en parcourant les pages de l'assistant d'installation ou en préparant un fichier de réponse. Par exemple, vous indiquez la langue de l'installation et le produit à installer, le type d'installation (installation rapide ou personnalisée) ainsi que les paramètres de configuration correspondants pour permettre l'exécution des composants installés.

Enfin, vous exécutez les instructions d'installation à l'aide des informations saisies à l'étape 2.

Vous pouvez installer et supprimer des composants de produit de manière interactive à l'aide de l'assistant d'installation. En outre, vous pouvez spécifier et modifier de nombreux paramètres et propriétés d'installation et de configuration via une interface de ligne de commande.

Présentation du programme d'installation

Le programme d'installation de Client Automation fournit des routines d'installation pour des fonctionnalités du produit standard et, éventuellement, d'autres produits CA Technologies sous forme de modules d'extension.

Les options d'installation rapide et personnalisée sont disponibles. Les installations rapides offrent une disponibilité rapide de certaines fonctionnalités de gestion, tandis que l'option d'installation personnalisée offre une grande souplesse et des options de sélection des fonctionnalités plus granulaires.

Vous pouvez sélectionner les fonctions de produit que vous avez acquises et procéder à leur installation rapide ou personnalisée. Tous les utilisateurs pourront sélectionner des fonctions de produit pour lesquelles ils n'ont pas acquis de licence pendant une période d'évaluation de 30 jours.

A l'aide de l'installation personnalisée du programme d'installation principal de Client Automation, vous pouvez installer le gestionnaire de MDB et le gestionnaire DSM pour des ordinateurs distants et locaux. Le programme d'installation est applicable aux MDB Microsoft SQL Server et Oracle.

Lorsque vous exécutez l'installation, le programme d'installation vérifie si la dernière MDB disponible est installée sur l'ordinateur cible. Si une MDB est déjà installée, le programme d'installation continue l'installation du gestionnaire DSM. Si aucune MDB n'est installée, le programme d'installation installe la MDB, puis le gestionnaire DSM. Le processus de vérification de l'installation de la MDB est également applicable lorsque vous procédez à une mise à niveau vers une version plus récente du gestionnaire DSM.

A l'aide du programme d'installation principal, vous pouvez également installer une MDB autonome Microsoft SQL Server ou Oracle sur des ordinateurs locaux ou distants. Toutefois, vous pouvez encore suivre le processus d'installation existant en installant la MDB d'abord, puis en installant le gestionnaire DSM.

Remarque : Si vous installez le gestionnaire DSM avec CCS sur une MDB distante, CCS doit déjà être installé avec une MDB sur l'ordinateur distant. Pour désinstaller le gestionnaire DSM, vous devez manuellement désinstaller CCS à partir de l'ordinateur distant.

Conditions requises et restrictions

Veuillez tenir compte des conditions requises et restrictions qui s'appliquent pour l'installation de Client Automation Version 12.9 :

- Vous devez posséder Microsoft SQL Server ou Oracle comme fournisseur de base de données.
- Pour Oracle, l'installation du gestionnaire nécessite la saisie du mot de passe "sys" de l'administrateur de la base de données lors de la phase interactive du programme d'installation. Pour SQL Server, les champs Administrateur DB et Mot de passe de l'administrateur DB sont masqués. Le programme d'installation utilise une connexion SQL Server approuvée pour installer la MDB et pour configurer le gestionnaire DSM.

Méthodes d'installation

Après avoir sélectionné les fonctionnalités du produit à installer, vous pouvez choisir la méthode d'installation et parcourir les invites pour démarrer la distribution et la configuration du produit.

Les méthodes d'installation suivantes sont disponibles :

Installation rapide

Installe un gestionnaire de domaine autonome, y compris un serveur de modularité, un agent et l'explorateur DSM sous Windows

Installation rapide de l'agent

Installe toutes les fonctions requises pour gérer un système final. Le gestionnaire de domaine ou serveur de modularité en charge de la gestion de ce système final devrait de préférence être déjà installé à un emplacement quelconque du réseau

Installation personnalisée

Vous permet de sélectionner ou de désélectionner des composants de produit individuels et de modifier les paramètres d'installation. Vous pouvez installer une MDB SQL Server ou Oracle sur des ordinateurs locaux et distants. Si le programme d'installation identifie une MDB compatible avec la version actuelle de CA ITCM sur l'ordinateur cible (local ou distant), l'installation de MDB est ignorée et l'installation de CA ITCM se poursuit.

Remarques sur l'installation

Tenez compte des remarques suivantes lors de l'installation de la MDB sur Oracle 11g :

- Au moins un client Oracle 11g doit être installé.
- Lors de l'installation d'un gestionnaire DSM avec une MDB Oracle, si vous choisissez d'installer le composant CCS, vous devez disposer d'un lecteur C: et ne pas modifier le chemin d'installation par défaut de ce composant.
- Client Automation prend en charge uniquement la méthode de connexion EZCONNECT du gestionnaire DSM à la base de données Oracle. Pour plus d'informations sur la configuration de la méthode de connexion EZCONNECT, consultez la documentation d'Oracle.
- Vous ne pouvez pas installer le gestionnaire DSM sur le même ordinateur que le serveur ou le client Oracle 11g 64 bits, car le client Oracle 11g 32 bits est requis. Si la MDB est installée sur un serveur Oracle 11g 64 bits, ce serveur doit être distant du gestionnaire DSM.
- IPv4 et IPv6 sont tous deux pris en charge entre le gestionnaire DSM et la MDB.
- Il est recommandé de disposer d'au moins 2 Go pour les zones SGA et PGA.
- Le journal d'installation est disponible dans le répertoire temporaire et nommé mdb-schema-setup.log.
- Lors d'une réinstallation ou d'une mise à niveau, saisissez les mots de passe sys, mdbadmin et ca_itrm corrects.
- Le package PIF de la MDB prend en charge l'installation autonome à partir d'un fichier de réponse sous Windows et Linux/Solaris.
- Si la base de données sous-jacente est Oracle, indiquez les informations d'identification de mdbadmin pour la connexion à la source de données. De plus, ajoutez le rôle AIADMIN à l'utilisateur mdbadmin avant d'exécuter l'extraction des données.

Informations complémentaires :

Conditions requises pour l'installation (page 118)

Remarques diverses sur l'installation

Lorsque les services Terminal Server Windows sont configurés en mode Serveur d'applications, les paramètres suivants sont requis :

- Utilisez le mode CONSOLE lors d'une installation à partir de l'accès distant.
  Exemple :

  mstsc /v:HostName /console

- Avant l'installation, modifiez les paramètres d'utilisateur Terminal Server par INSTALL.
  Exemple :
  change user /install

- Pour vérifier les paramètres d'utilisateur, exécutez la commande suivante :
  `change user /query`

Remarque : Pour en savoir plus sur l'utilitaire CHANGE USER de Windows Terminal Server, consultez l'article : support.microsoft.com/kb/186504/fr.

Informations complémentaires :

Conditions requises pour l'installation (page 118)

Remarques concernant l'installation liées au FIPS

Les remarques suivantes concernant d'installation s'appliquent à l'installation de Client Automation dans l'un des modes FIPS :

- Tous les composants DSM d'un ordinateur utilisent le même mode FIPS. Si, par exemple, vous installez un agent Asset Management sur un ordinateur déjà équipé de l'agent Software Delivery Version 12.9, il fonctionnera dans le même mode FIPS que ce dernier.
- Tous les composants de gestionnaire (moteur, services web, console web, générateur de rapports, etc.) doivent utiliser le même mode FIPS que le gestionnaire.
- Pour les déploiements mis en cluster, vous pouvez sélectionner le mode FIPS uniquement pour le premier noeud ; tous les autres noeuds fonctionnent dans le même mode que le premier noeud.

Sélection du mode FIPS lors de l'installation

Vous pouvez sélectionner le mode FIPS lors de l'installation interactive de Client Automation via le programme d'installation, ou de façon silencieuse via la ligne de commande, l'utilitaire msiexec ou le déploiement de l'infrastructure (DMDeploy). Le mode par défaut est Préférence-FIPS.

Remarque : Vous ne pouvez pas spécifier le mode FIPS lorsque vous mettez à niveau, modifiez ou réparez une installation de Client Automation. Vous pouvez modifier le mode FIPS des composants DSM après leur installation. Pour plus d'informations sur le basculement vers un mode FIPS particulier, consultez la section Fonctionnalités de sécurité.

Cette section décrit la procédure à suivre pour modifier le mode FIPS lors de l'utilisation de plusieurs méthodes et options d'installation :

Installation interactive

Lors de l'installation du produit, le programme d'installation Client Automation fournit une option de sélection du mode FIPS dans la section de conformité à la norme-FIPS. Pour activer le mode FIPS uniquement pour les composants que vous installez, sélectionnez cette case à cocher. Cette option n'est pas disponible lorsque vous modifiez ou que vous réparez une installation.

Remarque : Vous pouvez sélectionner le mode FIPS pendant une installation personnalisée uniquement. L'installation expresse installe toujours Client Automation dans le mode Préférence-FIPS. Dans le cas d'une installation d'un agent Remote Control autonome, vous pouvez spécifier le mode FIPS, que l'installation soit personnalisée ou expresse.

Installation via la ligne de commande, msiexec ou DMDeploy

Vous pouvez spécifier le paramètre suivant pour définir le mode FIPS lors d'une installation silencieuse à l'aide de la ligne de commande, de msiexec ou de DMDeploy :

Windows :

```
FIPS_MODE=1 //(FIPS-preferred)
FIPS_MODE=2 //(FIPS-only)
```

Linux ou UNIX :

```
/RITCM_FIPS_MODE=1 //(FIPS-preferred)
/RITCM_FIPS_MODE =2 //(FIPS-only)
```

Installation à l'aide de Software Delivery

Vous ne pouvez pas spécifier le mode FIPS lorsque vous utilisez Software Delivery pour installer ou mettre à niveau des composants DSM. Le mode FIPS est défini en fonction des facteurs suivants :

- Si la cible comprend déjà un composant DSM, toutes les installations ultérieures via Software Delivery utiliseront le même mode FIPS que le composant existant. Dans le cas contraire, le mode FIPS est défini sur Préférence FIPS.
- Remarque : Vous ne pouvez pas spécifier le mode FIPS lorsque vous modifiez ou que vous réparez une installation de Client Automation.

Dans tous les cas, le gestionnaire peut remplacer le mode FIPS en appliquant la stratégie de configuration qui définit le mode FIPS.

Installation de la migration automatisée

Conditions requises pour l'installation

Avant de lancer l'installation, vérifiez que les installations suivantes sont disponibles dans votre entreprise :

- CA IT PAM version 03.0.00 et Service Pack 03.0.01 ou CA Process Automation 03.1.00 et Service Pack 03.1.01 ou CA Process Automation 4.1 SP1.

  Remarque : De même, vous pouvez installer CA EEM pour la gestion des identités et des accès. Si vous voulez installer CA EEM dans un environnement Windows 64 bits, suivez les instructions figurant dans le fichier *EEM_Install_64.pdf*.

- Si vous utilisez une MDB Oracle et CA IT PAM version 03.0.00, vous devez installer le patch CA IT PAM, ITPAM_3.0_11182010_OracleJar_HF_19813962 avec CA IT PAM.

  Important : Avant d'appliquer le patch, arrêtez le service de l'orchestrateur CA IT PAM.

Remarques sur l'installation

Les remarques suivantes s'appliquent à la migration automatisée :

- La migration automatisée prend en charge les gestionnaires de domaines DSM et ne peut donc pas être appliquée à des gestionnaires d'entreprise DSM.
- La migration automatisée s'applique uniquement au gestionnaire de domaines par défaut lié à la console Web. Si la console Web est liée à plusieurs gestionnaires de domaines, la fonctionnalité de migration automatisée sera uniquement disponible une fois connectée au gestionnaire de domaines par défaut.
- Vous pouvez installer la migration automatisée uniquement sur une instance de console Web par gestionnaire de domaines. Si plusieurs instances de la console Web ont le même gestionnaire par défaut, vous devez installer la migration automatisée sur un seul des ordinateurs de la console Web.
- La migration automatisée est uniquement prise en charge sous des environnements d'exploitation Windows.
- Lorsque vous modifiez ou désinstallez la migration automatisée, si le gestionnaire WAC est installé sur un ordinateur distant, vérifiez que CAF est activé.

Configuration de la migration automatisée

Avant d'utiliser la migration automatisée, vous devez effectuer les tâches suivantes :

1. Configurez le compte d'utilisateur CA IT PAM dans Client Automation.
2. Activez le protocole SSL pour la console Web et les services Web d'automatisation.
3. (Facultatif) Modifiez le fichier de configuration du service d'automatisation.

Configurez le compte d'utilisateur CA IT PAM dans Client Automation.

La migration automatisée utilise CA IT PAM pour automatiser le flux de travaux de migration de système d'exploitation. Pour permettre à CA IT PAM d'interagir avec Client Automation, configurez un compte d'utilisateur CA IT PAM au niveau du gestionnaire de domaines DSM.

Remarque : L'utilisateur CA IT PAM que vous configurez doit disposer de droits d'exécution dans CA IT PAM.

Pour configurer le compte d'utilisateur de CA IT PAM dans Client Automation :

1. Créez un compte d'utilisateur WINNT local pour l'utilisateur CA IT PAM sur l'ordinateur du gestionnaire de domaines. Vous pouvez ignorer cette étape si vous voulez utiliser les informations d'identification d'utilisateur LDAP de l'utilisateur CA IT PAM.

   Important : La migration automatisée ne prend pas en charge Sun One Directory Server. Si vous utilisez Sun One Directory Server comme protocole LDAP, utilisez un compte d'utilisateur WINNT pour l'utilisateur CA IT PAM.

2. Ajoutez le compte d'utilisateur CA IT PAM aux profils de sécurité de Client Automation et accordez le contrôle total pour les classes d'objets de sécurité suivantes :

   - Job logiciel
   - Ordinateur
   - Conteneur de jobs logiciels
   - Image d'installation du système d'exploitation
   - Procédure
   - Groupe d'actifs
   - Requête commune
   - Gestionnaire
   - Informations d'identification de la base de données
   - Politique basée sur le logiciel
   - Groupe logiciel
   - Package logiciel

   L'administrateur de CA IT PAM est autorisé à accéder à Client Automation pour exécuter les fonctions nécessaires. Vous spécifiez les informations d'identification de cet utilisateur lors de la création des jobs de migration.

Configuration de l'accès à un partage DMM

Si le partage réseau DMM s'exécute sur Windows Server 2008 ou version supérieure, la procédure d'application DMM peut échouer avec une erreur d'exécution sur certains ordinateurs cibles pendant la phase de restauration.

Effectuez l'une des procédures suivantes :

- Utilisez un partage réseau DMM qui s'exécute sur Windows Server 2003 SP2.
- Utilisez un partage réseau DMM qui s'exécute sur Windows Server 2008 SP2 ou Windows Server 2008 R2, avec le protocole Server Message Block (SMB) 2.0 désactivé comme suit :
    1. Ouvrez Regedit.
    2. Accédez à HKLM, puis cliquez sur System, CurrentControlSet, Services, LanmanServer, Parameters.
    3. Ajoutez une clé DWORD avec le nom smb2 et définissez la valeur sur 0.
    4. Redémarrez le serveur.

Activation du protocole SSL pour la console Web et les services Web d'automatisation

L'activation de SSL (Secure Socket Layer) pour la console Web et les services Web d'automatisation leur permet de communiquer par le biais d'un canal sécurisé.

Procédez comme suit :

1. Suivez les instructions de la rubrique Activation du protocole SSL pour la console Web et les services Web dans l'Aide de la console Web.
2. Modifiez la valeur des paramètres suivants dans le fichier WACConfig.properties en plus des paramètres spécifiés dans la rubrique Activation du protocole SSL pour la console Web et les services Web de l'*Aide de la console Web DSM* :

    WIN7SERVICE_URL

    Définit l'URL du service Web d'automatisation. Modifiez l'URL pour démarrer avec https au lieu de http. Par exemple, https://testmachine.test.com/axis/services/automationService

    ITCMEPR

    Définit l'URL du service Web Client Automation. Modifiez l'URL pour démarrer avec https au lieu de http. Par exemple, https://testmachine.test.com/UDSM_R11_WebService/mod_gsoap.dll

3. Effectuez les instructions restantes de la rubrique Activation du protocole SSL pour la console Web et les services Web.

(Facultatif) Modification du fichier de configuration du service d'automatisation

Le fichier de configuration du service d'automatisation contient des paramètres de configuration que la migration automatisée utilise pour diverses tâches. Dans la plupart des cas, les paramètres par défaut contribuent à l'optimisation des performances de la migration automatisée. Toutefois, vous pouvez modifier certains paramètres pour améliorer les performances des jobs selon votre environnement, la charge que vos serveurs peuvent gérer, etc.

Pour modifier le fichier de configuration du service d'automatisation :

1. Ouvrez le dossier C:\Program Files\CA\DSM\Automation Service\bin ou le dossier %autohome%\bin.
2. Modifiez le fichier automation.config dans un éditeur de texte.
3. Modifiez la valeur des paramètres requis. Pour plus d'informations sur chaque paramètre, consultez la rubrique Fichier de configuration du service d'automatisation.

   Remarque : Un nombre entier dans le fichier automation.config ne doit pas contenir ni être entouré par des espaces. Lorsque vous spécifiez un nombre entier dans le fichier automation.config, vérifiez l'absence de tout espace dans la valeur et autour de cette dernière. Tout espace dans le nombre entier peut entraîner un dysfonctionnement du service d'automatisation.
4. Enregistrez le fichier et redémarrez Tomcat à l'aide des commandes suivantes :

   ```
   caf stop tomcat
   caf start tomcat
   ```

   Les modifications apportées au fichier de configuration prennent effet.

Installation multilingue

Au début de l'installation de Client Automation, une boîte de dialogue vous invite à choisir la langue de l'installation. Si votre environnement local utilise l'une des langues prises en charge, cette dernière est déjà présélectionnée comme langue par défaut. Si vous choisissez une autre langue, le programme d'installation s'exécute dans cette langue.

Afin de garantir la prise en charge de l'installation multilingue de CA Client Automation, le support d'installation (DVD) fournit le produit en plusieurs langues en plus de la version originale en anglais.

La langue dans laquelle vous choisissez d'exécuter le programme d'installation n'est pas forcément celle utilisée lors de l'utilisation du produit. Au cours de l'installation, vous serez invité à sélectionner les langues dans lesquelles le produit doit fonctionner ainsi que celles que vous souhaitez activer pour le produit dans les bibliothèques de logiciels Software Delivery et Déploiement de l'infrastructure.

Quelle que soit la langue choisie pour l'installation de Client Automation, CA Common Services (CCS) apparaît toujours en anglais.

Si aucun paramètre de langue n'est fourni (lors d'une installation autonome), l'environnement linguistique par défaut du système est utilisé, à condition que le package linguistique soit disponible. Si l'environnement linguistique par défaut du système ne figure pas parmi les langues prises en charge, le programme d'installation repasse à l'anglais (Etats-Unis).

Important : Pour prendre en charge des noms d'hôtes localisés, cela signifie, des noms d'hôtes qui sont en langues locales autres que l'anglais américain (non-ENU), il faut que l'infrastructure sous-jacente du DNS (système de nom des domaines) prenne en charge le codage à caractères UTF-8 dans le DNS.

Informations complémentaires :

Modification de la langue du produit après l'installation (page 217)

A propos de la création et de l'installation du package linguistique

CA Client Automation fournit des packages linguistiques de base indépendants pour l'agent d'inventaire matériel de base (BHI), l'agent Asset Management (AM), l'agent Remote Control (RC) et l'agent Software Delivery (SD). Le package linguistique indépendant en anglais (ENU) n'est pas fourni à part et est déjà inclus dans les packages de base.

Les administrateurs peuvent créer leur propre ensemble de packages d'agent à l'aide du script dsmPush et spécifier l'agent qu'ils veulent utiliser et dans quelle langue. Cette opération doit avoir lieu sur l'ordinateur du gestionnaire, après insertion du DVD dans l'unité de disque.

Le script dsmPush crée des unités d'installation qui contiennent un package linguistique de base indépendant destiné à l'agent, ainsi que les packages linguistiques souhaités. Si cela est indiqué dans la ligne de commande, dsmPush importe ces unités d'installation dans les bibliothèques de logiciels Software Delivery et Déploiement de l'infrastructure. En associant le paramètre "-single" au script dsmPush, l'administrateur peut forcer l'importation d'un seul package dans les bibliothèques.

Vous pouvez installer un package linguistique en même temps que le package de base ou par la suite, lors d'une opération à part. L'installation d'un package linguistique s'exécute de façon complètement autonome.

Nous vous conseillons d'enregistrer les packages linguistiques dans Software Delivery et Déploiement de l'infrastructure à l'aide du script dsmPush.

Remarque : Pour plus d'informations sur l'outil dsmPush, consultez le *Manuel de référence des composants CLI.*

L'installation de l'agent n'importe pas les packages vers la bibliothèque Déploiement de l'infrastructure ; seuls l'agent et un package linguistique sont installés (si vous n'installez pas la version anglaise). En revanche, si plusieurs packages d'agent multilingue sont déjà installés, le programme d'installation mettra à niveau les agents multilingues sans installer de package linguistique.

L'installation interactive offre un large choix de packages linguistiques pouvant être installés et dans lesquels le produit fonctionnera, qui seront importés dans les bibliothèques de logiciels Software Delivery et Déploiement de l'infrastructure.

Scénarios spéciaux d'installation des agents

La liste suivante fournit des informations utiles sur les scénarios spéciaux d'installation ou de mise à niveau des agents :

- **Procédures pour les agents sur les packages composés**

  Lorsque vous utilisez le script dsmPush pour créer des packages composés comprenant un ou plusieurs packages de base d'agent et plusieurs packages linguistiques, les seules procédures disponibles pour le package composé dans la bibliothèque de packages logiciels(disponible dans l'explorateur DSM, sous *Domaine*, Logiciel, Bibliothèque de packages logiciels, Packages logiciels, *Package*, Procédures) sont l'installation pour Linux, et l'installation et la désinstallation pour Windows.

  Pour exécuter une action particulière dans un produit (par exemple, la procédure Analyser SWD de la livraison logicielle), vous devez exécuter cette procédure à partir du package linguistique de base indépendant de l'agent dans la bibliothèque de packages logiciels.

- **Installation d'un agent autonome Remote Control**

  Il n'est pas possible d'installer un agent autonome Remote Control à l'aide des fonctions de Software Delivery, car l'agent de livraison logicielle doit être présent sur l'hôte de l'agent. (Un agent autonome de contrôle à distance doit fonctionner seul et ne peut coexister avec un autre module d'extension d'agent.)

  Pour installer un agent autonome de contrôle à distance, vous devrez soit l'installer de manière interactive, soit utiliser l'assistant Déploiement d'infrastructure et spécifier le paramètre supplémentaire /RITRM_RC_AGENT_STANDALONE=1. Ainsi, la procédure Agent autonome de l'agent de contrôle à distance n'est pas applicable au package composé dans la bibliothèque de packages logiciels.

Configuration matérielle requise

Les spécifications matérielles dépendent de nombreux paramètres, notamment l'architecture réseau, la bande passante disponible, la fréquence des opérations, la taille des opérations et le nombre de systèmes terminaux. Par exemple, si vous installez un gestionnaire Software Delivery, la quantité totale d'espace disque nécessaire dépend essentiellement de la taille et du nombre de packages logiciels et des images OSIM gérées.

Pour connaître la configuration matérielle minimale requise pour installer et utiliser CA Client Automation, consultez le chapitre Spécifications matérielles et configuration requise du *Fichier Readme de CA Client Automation*.

Base de données de gestion (MDB)

Le gestionnaire DSM requiert une base de données de gestion. Pour obtenir la liste actuelle des plates-formes prises en charge, consultez la matrice de compatibilité sur le site du support de CA.

Les MDB peuvent apparaître dans les configurations suivantes :

- **Configuration locale** - Le gestionnaire et la base de données sont exécutés sur le même ordinateur.

  Dans CA Client Automation, cela s'applique uniquement à une MDB basée sur Microsoft SQL Server. Le gestionnaire et la MDB sont tous deux installés dans un environnement d'exploitation Windows.

- **Configuration à distance** - La base de données est située sur l'ordinateur A et le gestionnaire est installé sur l'ordinateur B et utilise un client pour se connecter à la base de données sur l'ordinateur A.

  Dans CA Client Automation, cela s'applique à la fois aux MDB Microsoft SQL Server et Oracle.

  Pour une MDB Oracle, la configuration à distance est obligatoire. Actuellement, le gestionnaire DSM est installé sur un ordinateur exécutant Windows et la MDB Oracle est installée sur un ordinateur exécutant un système d'exploitations Sun Solaris pris en charge.

Dans l'architecture à plusieurs niveaux, les instances de la base de données de gestion (MDB) peuvent être implémentées au niveau du gestionnaire d'entreprise et de domaine. Ces deux niveaux prennent en charge les MDB Microsoft SQL Server et Oracle. Vous pouvez également implémenter les MDB sur différents fournisseurs de base de données sur les niveaux individuels. Par exemple, vous sélectionnez SQL Server pour le gestionnaire de domaine et Oracle pour le gestionnaire d'entreprise.

Dans les configurations mixtes, par exemple un gestionnaire de domaine avec une MDB basée sur SQL Server et un gestionnaire d'entreprise avec une MDB basée sur Oracle, vous avez besoin des clients de bases de données appropriés sur les gestionnaires ; dans cet exemple, vous avez besoin du client Oracle sur le gestionnaire de domaine et du client SQL sur le gestionnaire d'entreprise.

Avant de démarrer l'installation de CA Client Automation, le serveur de base de données (pour la configuration locale) ou le client de base de données (pour la configuration à distance) doit être installé.

Vous sélectionnez le type de base données au cours de l'installation de CA Client Automation.

Package PIF de la MDB

Vous pouvez utiliser ce package comme programme d'installation autonome de la MDB.

Installation autonome de la MDB

Vous pouvez appeler le package PIF de la MDB comme programme d'installation autonome de la MDB en exécutant le script d'installation (setup.bat ou setup.sh) à partir du répertoire de la MDB approprié :

```
<DVDROOT>\WindowsProductFiles_x86\mdb
```

```
<DVDROOT>/LinuxProductFiles_x86/mdb
```

```
<DVDROOT>/SolarisProductFiles_sparc/mdb
```

Le package PIF de la MDB utilisé comme programme d'installation autonome prend en charge les nouvelles installations de la MDB, les réinstallations et les mises à niveau sur un serveur de base de données cible local ou distant.

Pour Oracle, le package PIF autonome de la MDB vérifie si la version du client Oracle est Oracle 11g Release 2.

Enregistrements d'installation de PIF

Le programme d'installation de la MDB ne laisse aucun enregistrement d'installation de PIF sur l'ordinateur source appelé. En conséquence, vous pouvez réutiliser l'ordinateur source pour installer la MDB sur un autre ordinateur distant cible. Aucun enregistrement d'installation de PIF n'est conservé sur ce dernier.

Le programme d'installation de la MDB écrit, toutefois, son numéro de version dans la table ca_settings pour faciliter la maintenance.

Les anciens enregistrements d'installation de PIF sur l'ordinateur distant de la MDB ne sont pas supprimés lors d'une mise à niveau locale ou à distance de la MDB. Sur Solaris, vous pouvez supprimer ces anciens enregistrements d'installation manuellement à l'aide de la commande lsm -e.

Remarques concernant CCS

Il existe deux variantes de CA Common Services (CCS) installées avec CA Client Automation : une version réduite appelée Micro-CCS (uniquement en anglais) et la version complète originale. Micro-CCS (uniquement en anglais) prend en charge la Gestion des événements et les Calendriers, mais ne prend pas en charge WorldView (utilisé pour la configuration réseau DTS) ou Détection (y compris la détection continue). La version complète de CCS r11.2 (uniquement en anglais) peut uniquement être utilisée avec une MDB Microsoft SQL Server.

Le programme d'installation choisit automatiquement la variante appropriée au cours de l'installation. Notez que les deux variantes ne peuvent coexister sur un hôte unique, bien qu'elles puissent coexister sur plusieurs hôtes au sein d'un réseau. Sachez également que Micro-CCS ne peut pas être mis à niveau vers la version CCS complète.

Les tableaux ci-dessous résument quelle variante de CCS est installée avec les différents environnements d'exploitation et MDB :

Linux :

Composant installé	Variante CCS
Agent	Aucune
Serveur de modularité sans calendriers	Aucune
Serveur de modularité avec calendriers	Micro-CCS ; agent d'événements uniquement

Remarque : CA Client Automation n'utilise jamais la version CCS complète sous Linux.

Windows :

Composant installé	Variante CCS
Agent	Aucune
Serveur de modularité sans calendriers	Aucune
Serveur de modularité avec calendriers	Micro-CCS ; agent d'événements uniquement
*Gestionnaire avec MDB SQL Server locale	Version CCS complète
*Gestionnaire avec MDB SQL Server distante	Version CCS complète ; doit être installée sur l'hôte MDB et sur l'hôte Client Automation
Gestionnaire avec MDB Oracle distante	Micro-CCS sur hôte Client Automation uniquement ; agent d'événements plus gestionnaire d'événements

* Aucune différence avec ou sans mise en cluster

UNIX :

Aucune variante de CCS installée.

Remarque : Lors de l'installation d'un gestionnaire de domaines avec CCS, l'utilisation d'une instance nommée SQL Server entraîne l'échec de l'installation de CCS. Pour installer correctement CCS à l'aide d'une instance SQL nommée, vous devez exécuter le service Navigateur SQL Server. Vous pouvez lancer le service Navigateur SQL Server à partir du gestionnaire de configuration SQL Server.

Messages d'erreur d'installation CCS

L'installation des calendriers CCS est uniquement fiable avec un serveur de modularité. Les messages suivants peuvent apparaître lorsqu'une installation de la version CCS *complète* est exécutée avec un gestionnaire DSM. Tous les échecs mentionnés ont trait à l'interaction entre le CCS et une MDB basée sur un serveur SQL.

Texte d'erreur (dans %TEMP%\ TRC_Inst2_ITRM.log)	Conditions	Diagnostics et solutions
Le service MSSQLServer ne s'exécute pas sur \\hôte_local.	La MDB est distante ; les hôtes locaux et distants ne sont pas dans le même domaine.	Ce message est trompeur car aucun contact n'est établie avec l'hôte MDB distant. Ajoutez l'hôte local au même domaine que celui de l'hôte distant.
Le mot de passe saisi pour l'utilisateur nsmadmin n'est pas valide.		■ Le compte nsmadmin existe déjà dans SQL Server et le mot de passe spécifié lors de l'installation de DSM était différent. (a) Supprimez toutes les connexions DSM/CCS et utilisateurs DB de SQL Server avant de démarrer l'installation, ou (b) indiquez un mot de passe correspondant lors de l'installation de DSM, ou (c) modifiez le mot de passe nsmadmin dans SQL Server afin qu'il corresponde à la saisie effectuée au cours de l'installation de DSM. ■ Le mot de passe nsmadmin ne satisfait pas aux critères de force du mot de passe système. Renforcez le mot de passe.

Texte d'erreur (dans %TEMP%\ TRC_Inst2_ITRM.log)	Conditions	Diagnostics et solutions
Le service MSSQLServer ne s'exécute pas sur \\hôte_local.	La MDB est distante ; les hôtes locaux et distants ne sont pas dans le même domaine.	Ce message est trompeur car aucun contact n'est établie avec l'hôte MDB distant. Ajoutez l'hôte local au même domaine que celui de l'hôte distant.
Les informations de connexion à la MDB fournies ne sont pas valides.		Le compte nsmadmin a déjà été défini sur SQL Server ; la MDB peut exister ou non. Ce problème survient même si le mot de passe nsmadmin correspond à ce qui a déjà été paramétré dans SQL Server. Supprimez la ou les connexions DSM/CCS et le ou les utilisateurs DB de SQL Server afin que celui-ci soit vide.

Des processus actifs sont connectés à une ou plusieurs bases de données utilisées par ce produit. Pour garantir l'intégrité des données et la stabilité du système, fermez ces processus pour arrêter les connexions à la base de données avant de lancer l'installation.
[Dans %TEMP%\ITRM.CCS\wizint.log ou %TEMP%\DSM_CCS_wizint.log.]
		D'autres gestionnaires Client Automation distants partagent la MDB, par exemple :
		`11:36:50 ** Processus DB actifs **`
		`11:36:50 Processus DB pour`
		`11:36:50 DB Nom = mdb, Noeud = UNI6505L3-065, Processus = CA IT Client Manager r12`
		`11:36:50 DB Nom = mdb, Noeud = CMQA158, Processus = CA IT Client Manager r12`
		`11:36:50 Processus DB pour`
		`11:36:50 ** Fin des processus DB **`
		`11:36:50 Des processus actifs sont connectés...`
		En pratique, il est peu probable que cette situation se présente, à moins que l'ensemble du système Client Automation soit mal configuré ou configuré dans le mauvais ordre.
		Arrêtez temporairement les processus distants. Le fichier journal indique les hôtes distants qui sont impliqués.

Texte d'erreur (dans %TEMP%\ TRC_Inst2_ITRM.log)	Conditions	Diagnostics et solutions
Le service MSSQLServer ne s'exécute pas sur \\hôte_local.	La MDB est distante ; les hôtes locaux et distants ne sont pas dans le même domaine.	Ce message est trompeur car aucun contact n'est établie avec l'hôte MDB distant. Ajoutez l'hôte local au même domaine que celui de l'hôte distant.

Un test de vérification des dépendances a échoué.	Terminal Services est activé sur l'hôte.	Désactivez temporairement Terminal Services lors de l'installation de CCS. L'installation sur la console peut également fonctionner.
		Autrement, comme mentionné dans le manuel d'implémentation CCS/NSM, cette version prend en charge les installations via Windows Terminal Services même si le mode Serveur d'application est défini. Cependant, les paramètres suivants sont requis.
		■ Le mode CONSOLE doit être utilisé lors de l'installation à distance.
		Exemple :
		`mstsc /v:HostName /console`
		■ Les paramètres USER du serveur de terminaux doivent être modifiés sur INSTALL avant l'installation.
		Exemple :
		`change user /install`
		Pour vérifier les paramètres d'utilisateur, exécutez la commande suivante.
		`change user /query`
		Pour en savoir plus sur l'utilitaire CHANGE USER de Windows Terminal Server, consultez le site http://support.microsoft.com/kb/186504 http://support.microsoft.com/kb/186504.

Conditions requises pour l'installation du gestionnaire DSM

Il se peut que d'autres produits CA Technologies soient installés sur le système gestionnaire DSM, celui-ci ayant déjà installé une MDB.

Avant de commencer une installation du gestionnaire DSM, assurez-vous qu'aucun autre produit n'utilise la MDB. Si un autre produit utilise la MDB, le processus d'installation se bloquera probablement.

Sous Windows, si vous souhaitez installer Client Automation après Unicenter Asset Portfolio Management, vérifiez si le processus corasmm.exe est en cours d'exécution. Si tel est le cas, configurez le serveur de notification Unicenter Asset Portfolio Management et le service de cache Unicenter Asset Portfolio Management en mode manuel, puis redémarrez l'ordinateur avant d'installer Client Automation. Lorsque l'installation Client Automation est terminée, redémarrez et réactivez les deux services Unicenter Asset Portfolio Management. Cette opération peut être effectuée à partir du gestionnaire de contrôle des services, via Panneau de configuration, Outils d'administration, Services.

Considérations relatives à l'espace disque pour l'installation du gestionnaire de la MDB

Installez le gestionnaire DSM sur une partition disposant d'au moins 12 Go d'espace libre. L'installation proprement dite utilise environ 7,7 Go d'espace disque, sans compter l'espace pour les fichiers journaux. Si la MDB est également installée sur cette partition, vous devez réserver au moins 50 Go supplémentaires pour la base de données (SQL Server et Oracle) et les fichiers journaux et fichiers de point de contrôle en ligne associés. Une base de données SQL Server ou Oracle de grande taille peut nécessiter jusqu'à 100 Go d'espace disque. Ces chiffres dépendent de vos besoins en termes de stockage de données, pour le stockage des packages logiciels en vue de leur distribution. Pour plus d'informations, consultez le chapitre Spécifications matérielles et configuration requise des *Notes de parution CA Client Automation* fournies avec la documentation CA Client Automation (bibliothèque).

Aucun redémarrage du système n'est normalement nécessaire après l'installation, mais cela peut améliorer les performances, davantage de ressources système étant alors disponibles.

La taille de la base de données tempdb doit être suffisante pour permettre la réplication de données entre le niveau domaine et le niveau entreprise. Par conséquent, il est important de disposer de suffisamment d'espace pour les fichiers tempdb et le journal de transaction. Nous vous conseillons de définir la taille initiale du fichier tempdb au niveau du domaine à 80 Mo et au niveau de l'entreprise à 2 Go. En outre, assurez-vous que la propriété de croissance automatique est définie sur "mode de croissance illimitée".

Gestionnaire autonome dans un environnement de base de données mixte

Si vous êtes sur le point d'installer un gestionnaire de domaines autonome et que vous voulez ensuite le relier à un gestionnaire d'entreprise qui utilise un type de base de données MDB différent, vous devez installer manuellement le client de base de données approprié sur le gestionnaire de domaines. Cela permet au gestionnaire de domaines de se connecter au gestionnaire d'entreprise pour la réplication.

Si, par exemple, votre gestionnaire de domaines utilise Microsoft SQL Server et que le gestionnaire d'entreprise utilise Oracle, vous devez installer le client de base de données Oracle sur le gestionnaire de domaines.

Installation autonome d'une MDB à l'aide d'un fichier de réponse

Le programme d'installation de MDB prend en charge l'installation autonome à partir d'un fichier de réponse à l'aide de la commande setup.bat -r response_file sous Windows et setup.sh -r response_file sous Linux/Solaris.

Le programme d'installation de MDB prend également en charge la création d'un fichier de réponse à l'aide de la commande setup.bat -g response_file sous Windows et setup.sh -g response_file sous Linux/Solaris.

Au lieu de générer un fichier de réponse, vous pouvez modifier le modèle de fichier de réponse (install.rsp) et l'utilisation pour effectuer une installation autonome.

Chiffrement et déchiffrement de mots de passe dans un fichier de réponse

Par défaut, les programmes d'installation de MDB utilisent le chiffrement Blowfish et l'utilitaire de déchiffrement inclus dans les packages de MDB : blfs.exe sous Windows et blfs sous Linux et Solaris. Si vous exécutez l'installation avec l'option -g, l'application utilisera automatiquement Blowfish pour chiffrer les mots de passe dans le fichier de réponse.

Si vous créez le fichier de réponse en modifiant le modèle inclus (install.rsp), exécutez l'utilitaire Blowfish à partir d'une fenêtre de commande ou de shell pour chiffrer le mot de passe. Puis, copiez la chaîne résultante dans le fichier de réponse.

Par exemple, si la commande blfs validation_0101 sous Linux/Solaris renvoie la chaîne chiffrée, 0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673, vous devez copier cette chaîne dans le fichier de réponse comme suit :

```
# Password of Oracle MDB admin user
ITRM_MDBADMINPWD=0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673
```

Dans les deux cas, lorsque vous exécutez l'installation avec l'option -r, l'application utilise automatiquement l'utilitaire Blowfish pour déchiffrer des mots de passe dans le fichier de réponse.

Remarque : Les mots de passe non chiffrés ne peuvent pas commencer par 0x (sensible à la casse).

L'algorithme Blowfish n'est pas conforme à la norme FIPS. Vous pouvez fournir un utilitaire conforme à la norme FIPS personnalisé pour le chiffrement ou le déchiffrement en définissant des variables d'environnement pointant vers les programmes pertinents. En d'autres termes, définissez MDB_ENC_PROG sur le nom du chemin complet du programme de chiffrement et MDB_DEC_PROG sur le nom du chemin complet du programme de déchiffrement.

Exemple : Modification des programmes de chiffrement ou de déchiffrement sous Windows

```
Définissez MDB_ENC_PROG sur E:\tmp\my_encrypter.exe.
```

```
Définissez MDB_DEC_PROG sur E:\tmp\my_decrypter.exe.
```

Sous Windows, les noms de fichier des programmes doivent avoir l'extension .exe.

Exemple : Modification des programmes de chiffrement ou de déchiffrement sous Solaris ou Linux

```
MDB_ENC_PROG : /tmp/my_encrypter
export MDB_ENC_PROG
```

```
MDB_DEC_PROG : /tmp/my_decrypter
export MDB_DEC_PROG
```

Si vous ne définissez pas MDB_DEC_PROG, ou si le programme n'existe pas, MDB_DEC_PROG sera considéré identique à MDB_ENC_PROG. Si vous ne définissez pas MDB_ENC_PROG ou si le programme n'existe pas, les programmes de chiffrement et de déchiffrement Blowfish par défaut seront utilisés.

Préparation du travail avec la MDB Microsoft SQL Server

Avant d'installer un gestionnaire DSM basé sur Microsoft SQL Server, SQL Server doit avoir été installé avec la configuration suivante :

- L'authentification en mode mixte (c'est-à-dire, l'authentification Windows et SQL Server) est requise
- Le protocole réseau TCP/IP est activé et opérationnel. Pour plus d'informations sur le choix et la configuration des protocoles réseau, consultez la documentation sur SQL Server.
- La règle suivante s'applique au regroupement serveur sélectionné au cours de l'installation de SQL Server :

  Vous devez choisir un nom de regroupement non sensible à la casse.

Utilisez l'assistant d'installation de Client Automation et suivez les instructions de configuration de la MDB SQL Server :

- Sur la page "Configurer le gestionnaire" de l'assistant, vous devez saisir les spécifications obligatoires (paramètres de connexion) pour le système de base de données cible, tels que :
  - Fournisseur de la base de données de gestion (sélectionnez le serveur SQL Microsoft)
  - Serveur de la base de données de gestion
  - Mot de passe MDB

    Remarque : Du fait de l'utilisation de l'authentification en mode mixte, ce mot de passe doit être conforme au niveau de sécurité d'un mot de passe de connexion système.

- Sur la page "Configurer la MDB Microsoft SQL Server", vous pouvez saisir les paramètres de configuration suivants :
  - Mode de compatibilité

    Remarque : La case Mode de compatibilité doit être cochée si vous êtes sur le point d'installer une nouvelle MDB 1.5 fournie avec le produit et que vous prévoyez d'installer ultérieurement un autre produit CA Technologies prenant uniquement en charge la MDB 1.0.4. Si la case Mode de compatibilité n'est pas cochée, l'installation de tout autre produit ne prenant pas en charge la MDB 1.5 échouera.

    Par défaut : le mode de compatibilité n'est pas sélectionné.
  - Nom de la base de données MDB

    Par défaut : mdb
  - Nom de l'instance MDB.

    Dans la liste déroulante, sélectionnez le nom de l'instance.

    Valeur par défaut : par défaut
  - Numéro de port de la base de données

    Valeur par défaut : 1433

Lors de l'installation, vous devez entrer le numéro de port associé à l'instance Microsoft SQL Server pour toutes les instances autres que celles par défaut. Le port peut être recherché dans la configuration TCP/IP SQL Server à l'aide du gestionnaire de configuration SQL Server.

Si Microsoft SQL Server est configuré à l'aide d'instances nommées, l'option "Ports dynamiques TCP" est automatiquement activée avec le numéro de port (configuration de port dynamique). Cependant, le gestionnaire de domaine ou d'entreprise ne parvient pas toujours à accéder à la base de données, car le numéro de port sur le système de la MDB a été modifié (par exemple, à la suite d'un redémarrage du système). Pour éviter ces échecs d'accès, nous vous recommandons de remplacer manuellement le paramètre du port par un ID de port statique, comme suit :

- Dans le menu Démarrer de Windows, ouvrez Gestionnaire de configuration SQL Server, Configuration du réseau SQL Server, Protocoles pour *nom_instance*, TCP/IP.
- Cliquez avec le bouton droit de la souris et sélectionnez Propriétés dans le menu contextuel.
- Dans la boîte de dialogue Propriétés TCP/IP, sélectionnez l'onglet Adresses IP. Dans la zone IPAll, coupez la valeur du port affichée dans le champ Ports TCP dynamiques et collez-la dans le champ Port TCP.

Important : Si vous attribuez manuellement un numéro de port autre que celui par défaut, nous vous recommandons de mettre à jour la liste reservedPorts dans le registre. Dans le cas contraire, le CAF pourrait démarrer avant SQL Server après le redémarrage ; si le CAF lance une requête de numéro de port dynamique, il pourrait obtenir le numéro de port défini pour SQL Server. SQL Server pourrait alors ne pas parvenir à démarrer.

Installation du gestionnaire DSM : MDB Microsoft SQL Server

Après l'installation de la MDB Microsoft SQL Server, installez le gestionnaire d'entreprise ou de domaines DSM.

Procédez comme suit :

1. Installez le client Microsoft SQL sur l'ordinateur sur lequel vous voulez installer le gestionnaire d'entreprise ou de domaines DSM.

   Remarque : Si Microsoft SQL Server est déjà installé sur l'ordinateur, cette étape n'est pas nécessaire.

2. Installez le gestionnaire DSM Client Automation et indiquez les détails de la MDB Microsoft SQL Server dans les boîtes de dialogue pertinentes.
3. Démarrez CAF.

Installation distante de la MDB pour Microsoft SQL Server

Si vous prévoyez d'exécuter le gestionnaire DSM avec une MDB distante Microsoft SQL Server, l'ordinateur du gestionnaire et l'ordinateur de la MDB distante doivent présenter une relation de confiance lors de l'exécution dans un environnement Windows.

Au cours de l'installation d'un gestionnaire de domaines ou d'entreprise, vous avez le choix entre installer la MDB sur l'hôte local ou utiliser une instance distante existante de la MDB.

Pour une configuration à distance, installez la base de données sur l'ordinateur distant en sélectionnant Installer la MDB (non la fonctionnalité CCS).

Si vous devez utiliser CCS avec Client Automation, vous devez installer CCS sur l'ordinateur hôte de la MDB, local ou distant. Dans la boîte de dialogue d'installation Client Automation de niveau supérieur, utilisez l'option Installer CCS. Puis, installez le gestionnaire de domaines ou d'entreprise.

Si vous utilisez une MDB Microsoft SQL Server distante, installez les outils de gestion de client Microsoft SQL *avant* d'installer le gestionnaire de domaines ou d'entreprise. Veillez à ce que les outils de gestion client Microsoft SQL ne sont pas désélectionnés au cours de l'installation du client Microsoft SQL.
Client Automation emploie l'utilisateur ca_itrm spécifique créé au niveau de la base de données afin d'être authentifié pour l'accès à la MDB. Le même mot de passe de l'utilisateur ca_itrm doit être indiqué dans les boîtes de dialogue d'installation de la MDB et d'installation Client Automation. L'utilisateur ca_itrm est créé automatiquement.
Lorsque vous installez plusieurs gestionnaires de domaines avec des MDB Microsoft SQL Server distantes, vérifiez qu'une seule MDB existe sur chaque instance du serveur de base de données. Cette restriction signifie que vous devez disposer d'autant de serveurs de base de données que de MDB.

Remarque : Avec une MDB Microsoft SQL Server distante, le nom du serveur hébergeant le domaine de la MDB est utilisé comme le nom du gestionnaire de domaines. Par conséquent, l'explorateur DSM dans le gestionnaire d'entreprise affiche le gestionnaire de domaines avec le nom de son serveur de base de données.

Préparation du travail avec une MDB Oracle

Utilisez l'assistant d'installation de Client Automation pour configurer le gestionnaire à utiliser avec une MDB Oracle, comme décrit ci-dessous. Il est essentiel que les valeurs des paramètres indiquées au cours de ces étapes de configuration correspondent aux valeurs saisies lors de l'installation de la MDB Oracle :

- Sur la page "Configurer le gestionnaire" de l'assistant, vous devez saisir les spécifications obligatoires (paramètres de connexion) pour le système de base de données cible, tels que :
  - Fournisseur de la MDB (sélectionnez Oracle)
  - Serveur MDB :
  - Mot de passe MDB
  - Administrateur de la base de données (sys)

    (Pour plus d'informations, consultez Utilisateur administrateur de la base de données sur Oracle (page 140).)
  - Mot de passe de l'administrateur de la base de données
- Cliquez sur le bouton Base de données dans la zone Configuration avancée du gestionnaire pour ouvrir une autre page de l'assistant et indiquer les paramètres de configuration avancée pour une installation personnalisée de la MDB.
- Sur la page "Configurer la MDB Oracle", vous pouvez définir les paramètres de configuration avancée suivants :
  - Mode de compatibilité

    Remarque : La case Mode de compatibilité doit être cochée si vous êtes sur le point d'installer une nouvelle MDB 1.5 fournie avec le produit et que vous prévoyez d'installer ultérieurement un autre produit CA Technologies prenant uniquement en charge la MDB 1.0.4. Si la case Mode de compatibilité n'est pas cochée, l'installation de tout autre produit ne prenant pas en charge la MDB 1.5 échouera.

    Par défaut : le mode de compatibilité n'est pas sélectionné.
  - Nom de la base de données MDB

    Par défaut : orcl
  - Numéro de port de la base de données

    Valeur par défaut : 1521
  - Mot de passe de l'administrateur de la MDB

Configuration requise

Cette section décrit la configuration requise pour l'installation de la MDB sur Oracle 11g :

- Installez le serveur Oracle 11g sur l'ordinateur sur lequel vous prévoyez d'installer ou de mettre à niveau la MDB. Cette version prend en charge les serveurs Windows, Solaris et Linux pour une MDB Oracle 11g.
- Créez une instance Oracle à l'aide de l'assistant de configuration de base de données Oracle. Tenez compte des facteurs suivants lors de la création de l'instance :
  - Le nom de l'instance de base de données (SID) doit être identique à celui du service Oracle (nom global).
  - Les valeurs appropriées doivent être saisie dans les champs SGA Size et PGA Size de l'onglet Memory de l'assistant de configuration de base de données Oracle.

    Il est recommandé de disposer d'au moins 2 Go pour SGA.
- Installez le client Oracle 11g sur l'ordinateur sur lequel vous prévoyez d'installer ou de mettre à niveau le gestionnaire DSM de CA ITCM.

Remarque : Pour des instructions d'installation détaillées, consultez le Manuel d'installation disponible dans la bibliothèque de documentation Oracle.

Utilisateur administrateur de la MDB sur Oracle

L'installation du gestionnaire nécessite l'intervention d'un Utilisateur administrateur Oracle. Si vous utilisez l'utilisateur Oracle "SYS", le programme d'installation se connectera "en tant que sysdba". Vous pouvez toutefois utiliser un autre utilisateur ; dans ce cas, l'utilisateur doit être créé en tant qu'utilisateur bénéficiant des mêmes privilèges que SYSDBA. En d'autres termes, les privilèges SYSDBA sont octroyés à cet utilisateur.

Les opérations suivantes effectuées sur Oracle nécessitent des privilèges SYSDBA :

- Démarrer une base de données
- Arrêter une base de données
- Sauvegarder une base de données
- Récupérer une base de données
- Créer une base de données

Installation d'une MDB Oracle (autonome)

Important : Notez les valeurs et mots de passe que vous saisissez au cours des étapes suivantes, car vous en aurez besoin pour configurer le gestionnaire DSM.

Les étapes de base pour l'installation de la MDB sur Oracle 11g en mode interactif sont les suivantes :

1. Si vous ne l'avez pas encore fait, créez une instance Oracle à l'aide de l'assistant de configuration de base de données Oracle et procédez comme suit :
   - Vérifiez que nom de l'instance de base de données (SID) est identique à celui du service Oracle (nom global).
   - Saisissez des valeurs appropriées pour l'instance dans les champs SGA Size et PGA Size dans l'onglet Memory de l'assistant de configuration de base de données Oracle.
2. A partir du répertoire de la MDB, exécutez le fichier de script approprié sur le serveur de base de données cible :

   (Applicable à Windows)

   ```
   setup.bat
   ```

   (Applicable à Solaris et Linux)

   ```
   sh ./setup.sh
   ```

   Le programme d'installation de la MDB est lancé et la première page de l'assistant Sélectionner la langue d'installation s'affiche.
3. Acceptez l'anglais comme langue d'installation.

   Remarque : La seule langue disponible pour cette version est l'anglais.
4. Acceptez le contrat de licence de l'utilisateur final.
5. (Windows uniquement) Pour cette procédure, sélectionnez le type de base de données, Serveur Oracle.
6. Pour définir l'environnement d'exécution et de travail Oracle, dans le champ ORACLE_HOME, saisissez le chemin d'accès à l'installation Oracle le la MDB.

   Pour l'installation de la MDB distante, saisissez la valeur ORACLE_HOME de votre ordinateur local.
7. Spécifiez le nom du serveur de base de données Oracle et la taille de la MDB.
8. Spécifiez l'utilisateur de la MDB et les informations d'identification de l'administrateur de base de données.

   Remarque : Par défaut, le nom d'utilisateur de la MDB est ca_itrm.

9. Spécifiez des paramètres avancés de configuration Oracle, notamment le nom de service Oracle, le nom du Transparent Network Substrate (TNS) d'Oracle, le numéro de port, le chemin d'accès à l'espace disque logique et le mot de passe de l'administrateur de la MDB.

10. Pour vérifier les options de configuration de la base de données et confirmer l'installation, cliquez sur le bouton Installer.

    L'installation commence et le schéma de la MDB est créé dans la base de données Oracle.

    Remarque : Sous Solaris, le programme d'installation de la MDB affiche une boîte de dialogue contenant les vérifications de la version Oracle et des conditions préalables de l'environnement d'exploitation. Dans le nouveau programme d'installation de la MDB, cette boîte de dialogue s'affiche uniquement en cas d'échec des conditions préalables ; dans le cas contraire, l'installation se poursuivra.

11. A l'issue de l'installation de la MDB Oracle, installez le gestionnaire DSM.

Remarque : Le gestionnaire DSM utilise EZCONNECT pour la connexion à la MDB Oracle.

Installation du gestionnaire DSM : MDB Oracle

Installez le gestionnaire de l'entreprise ou de domaines DSM.

Procédez comme suit :

1. Installez le client Oracle 11g sur l'ordinateur sur lequel vous voulez installer le gestionnaire d'entreprise ou de domaines DSM.
2. Installez le gestionnaire DSM Client Automation et indiquez les détails de la MDB Oracle dans les boîtes de dialogue pertinentes.

   Remarque : Lorsque l'installation de gestionnaire requiert le nom du serveur Oracle de la MDB, saisissez l'adresse IP uniquement si le gestionnaire et la MDB sont sur le même ordinateur. Sinon, entrez l'hôte ou le nom DNS.
3. Pour terminer l'installation du gestionnaire, suivez les invites de l'assistant.
4. Si le gestionnaire DSM est installé sur le même ordinateur que la MDB Oracle pour Windows, effectuez les étapes supplémentaires suivantes :
   a. Exécutez la commande SQL suivante en tant que mdbadmin :

   ```
   update ca_n_tier set
           label='<MDB Server host name>',
           db_host_name='<MDB Server host name>',
           db_server='<MDB Server DNS name>'
   where domain_uuid in (select set_val_uuid from ca_settings where
   set_id=1)
   ```

   b. Vérifiez que la mise à jour est validée. Si la validation automatique est désactivée, validez la mise à jour manuellement.

   c. Dans l'invite de commande, exécutez la commande suivante.

   ```
   ccnfcmda -cmd setparametervalue -ps /itrm/database/default -pn dbmsserver
   -v <MDB Server DNS name>
   ```
5. Démarrez CAF.

Installation d'une MDB Oracle distante

Pour installer une MDB Oracle distante, créez d'abord une instance Oracle à l'aide de l'Assistant de configuration de la base de données Oracle sur un ordinateur distant fonctionnant avec un système d'exploitation Sun Solaris.

Pour installer la MDB Oracle

1. Connectez-vous à l'hôte Solaris en tant qu'utilisateur "racine" et naviguez vers *DVD_mount*/SolarisProductFiles_MDB/remotemdb.
2. Lancez sh ./setup.sh
3. Sélectionnez Choisir la langue.

   L'assistant d'installation est disponible en plusieurs langues : l'anglais, le français, l'allemand et le japonais.
4. Sélectionnez Nouvelle instance puis suivez les instructions de l'assistant.

   Important : Notez les valeurs et mots de passe que vous entrez au cours des étapes suivantes, car vous en aurez besoin pour configurer le gestionnaire DSM.
5. Lisez et acceptez le contrat de licence de l'utilisateur final pour poursuivre l'installation.
6. Pour la variable de l'environnement ORACLE_HOME, saisissez le chemin de l'installation Oracle que vous souhaitez utiliser pour la MDB.

   Le programme d'installation examine la plate-forme matérielle et l'environnement ORACLE. Si un test échoue, l'installation n'a pas lieu. Si tous les tests réussissent, l'installation peut continuer.
7. Sélectionnez un "nom d'instance de produit" pour l'installation en cours. Il s'agit en général du nom de l'instance ORACLE (SID).

   La liste déroulante Sélection du nom du produit présente les noms déjà utilisés. Le nom que vous choisissez doit être unique.
8. Entrez le mot de passe associé au nom d'utilisateur de la MDB (ca_itrm).

   Ce mot de passe se définit au moment de l'installation et sa confirmation est demandée. Mémorisez le mot de passe.
9. Entrez le nom de l'administrateur DB (le nom par défaut est "sys") et le mot de passe de l'administrateur DB. L'administrateur DB est un *nom d'utilisateur* auquel le privilège SYSDBA a été attribué dans l'instance Oracle.

   Remarque : Pour plus d'informations, consultez le document *Présentation de la MDB* dans la documentation Client Automation (Bibliothèque).

10. Indiquez si vous souhaitez installer le mode de compatibilité.

    Remarque : La case Mode de compatibilité doit être cochée si vous êtes sur le point d'installer une nouvelle MDB 1.5 fournie avec le produit et que vous prévoyez d'installer ultérieurement un autre produit CA Technologies prenant uniquement en charge la MDB 1.0.4. Si la case Mode de compatibilité n'est pas cochée, l'installation de tout autre produit ne prenant pas en charge la MDB 1.5 échouera.

    Par défaut : le mode de compatibilité n'est pas sélectionné.

11. Dans le champ Base de données MDB, entrez l'ID de session de l'instance de la base de données Oracle que vous souhaitez utiliser pour la MDB.

    La valeur par défaut de ce champ est le nom de l'instance de produit saisi à la page précédente de l'assistant.

12. Indiquez le numéro de port de la base de données.

    Valeur par défaut : 1521

    Important : Le numéro de port à indiquer ici dépend du numéro de port utilisé lors de la création de la base de données. Si un numéro de port autre que celui par défaut a été utilisé au moment de la création de la base de données, alors le même numéro de port doit être spécifié lors de l'installation de la MDB. Sinon, ne modifiez pas le numéro de port par défaut de la base de données.

13. Saisissez le chemin de l'espace de la table, c'est-à-dire le répertoire dans lequel Oracle crée les fichiers de la base de données. Tous les répertoires de ce chemin doivent déjà exister, à l'exception du dernier. Par exemple, dans le chemin par défaut prédéfini dans l'assistant, le répertoire "mdb" n'a pas besoin d'exister.

    Valeur par défaut : /opt/CA/SharedComponents/oracle/mdb

14. Dans le champ Mot de passe de l'administrateur de la MDB, vous devez indiquer le mot de passe de l'utilisateur MDBADMIN.

    L'utilisateur de la base de données MDBADMIN sert à créer le schéma de la MDB et devient le propriétaire de ce dernier.

15. A la page Installer MDB de l'assistant, confirmez l'installation en cliquant sur Installer.

    Après cette confirmation, le schéma de la MDB est créé dans la base de données Oracle.

Important : Si vous utilisez une MDB Oracle distante, un client Oracle 11*g* doit être disponible sur le gestionnaire et sur chaque système exécutant un moteur DSM ou le générateur de rapports DSM. Assurez-vous que le client Oracle 11*g* de type "Administrateur" est bien installé.

Informations complémentaires :

Maintenance de la MDB Oracle (page 220)

Installation distante de la MDB pour Oracle

Remarque : L'installation distante de la MDB sur une base de données Oracle est uniquement prise en charge par Windows.

Pour une installation distante, la variable d'environnement ORACLE_HOME fait référence à l'ordinateur local (sur lequel vous pouvez disposer d'un seul client Oracle).

Pour effectuer une installation et des mises à niveau vers une MDB Oracle distant, définissez un nom TNS pour l'ordinateur distant dans le fichier tnsnames.ora Oracle sur l'ordinateur local. Cela permet au serveur distant Oracle d'être traité.

Lors d'une installation de la MDB Oracle locale, le programme d'installation de MDB crée le dossier de chemin d'accès à l'espace disque logique spécifié s'il n'existe pas. Cette étape ne s'applique pas à une installation distante. Par conséquent, vérifiez que le chemin d'accès au dossier de l'espace disque logique que vous allez sélectionner lors de l'installation de la MDB existe sur l'ordinateur distant. Si le dossier de l'espace disque logique n'existe pas sur l'ordinateur distant, une erreur se produira et empêchera l'installation de se poursuivre.

Remarque sur la prise en charge CCS pour Oracle

CA Common Services (CCS) ne prend actuellement pas en charge une MDB Oracle.

Par conséquent, dans Client Automation, un sous-ensemble CCS est disponible avec un nombre réduit de fonctionnalités, concentré exclusivement sur les besoins de Client Automation, essentiellement la prise en charge des événements (calendrier) et d'IPv6.

Le programme d'installation sélectionnera automatiquement la version de CCS adaptée à votre environnement.

Remarques concernant l'installation et la configuration de la MDB Oracle

La section suivante décrit l'installation et la configuration de la MDB Oracle.

Installation du serveur Oracle sous Solaris

Pour des instructions d'installation détaillées, consultez le Manuel d'installation disponible dans la bibliothèque de documentation Oracle.

Suppression et recréation d'une instance de base de données Oracle

Utilisez l'assistant de configuration de la base de données Oracle pour supprimer une instance de base de données Oracle et en créer une nouvelle. Lorsque vous créez une instance de base de données Oracle à l'aide de cet outil, vous devez saisir la taille de la mémoire qu'Oracle peut utiliser pour cette instance. Entrez les valeurs de taille appropriées dans les champs SGA Size et PGA Size de l'onglet Memory.

Par exemple, saisissez 1198 dans le champ SGA Size et 399 dans le champ PGA Size. Ces valeurs suggérées offrent environ 1,2 Go de mémoire pour les données et les informations de contrôle (SGA) et environ 0,4 Go pour la zone des programmes (PGA). Il s'agit des valeurs minimales recommandées pour une installation contenant un maximum de 10 000 actifs informatiques.

Vérification de l'installation du serveur Oracle

Vous devez disposer de la version Oracle et du niveau de patch appropriés ; sinon, les opérations du gestionnaire DSM risquent d'échouer. Pour vérifier la version Oracle et le niveau de patch, exécutez la commande suivante :

```
goto $ORACLE_HOME/OPatch
call ./opatch lsinventory
```

Configuration de la MDB Oracle pour une prise en charge des langues à plusieurs octets

Lorsque vous créez une instance de base de données Oracle à l'aide de l'assistant de configuration de la base de données, sélectionnez l'option Use Unicode (AL32UTF8) dans l'onglet Character Sets afin de prendre en charge les langues à plusieurs octets.

Modifier le mot de passe par défaut pour l'utilisateur ca_itrm

Lors de l'installation du gestionnaire ou de la MDB, vous pouvez modifier le mot de passe pour l'utilisateur ca_itrm utilisé pour accéder à la MDB.

Pour remplacer le mot de passe ca_itrm par un autre de votre choix, vous devez suivre plusieurs étapes, en fonction de l'un des fournisseurs de base de données suivants :

- MDB Microsoft SQL Server
- base de données de gestion Oracle

Modification du mot de passe par défaut lors de l'utilisation de Microsoft SQL Server

Si vous souhaitez remplacer le mot de passe par défaut pour l'utilisateur ca_itrm par l'un de votre choix lors de l'utilisation de Microsoft SQL Server comme fournisseur de base de données, procédez comme suit

1. Accédez au système sur lequel Microsoft SQL Server est en cours d'exécution.
2. Ouvrez Démarrer, Programmes, Microsoft SQL Server Management Studio.
3. Sélectionnez l'utilisateur ca_itrm dans le Management Studio et modifiez le mot de passe.
4. Accédez au système sur lequel le gestionnaire a été installé.
5. Exécutez cadsmcmd setDBCredentials passwd=*nouveau_mot_de_passe*.
6. Exécutez caf stop.
7. Exécutez caf start.

Modification du mot de passe par défaut lors de l'utilisation d'Oracle

Si vous souhaitez remplacer le mot de passe par défaut pour l'utilisateur ca_itrm par l'un de votre choix lors de l'utilisation d'Oracle comme fournisseur de base de données, procédez comme suit

1. Accédez au système sur lequel Oracle est en cours d'exécution.
2. Ouvrez Démarrer, Programmes et lancez le programme Oracle Database Control approprié.
3. Sélectionnez l'utilisateur ca_itrm dans Oracle Database Control et modifiez le mot de passe.
4. Accédez au système sur lequel le gestionnaire a été installé.
5. Exécutez cadsmcmd setDBCredentials passwd=*nouveau_mot_de_passe*.
6. Exécutez caf stop.
7. Exécutez caf start.

Fichiers journaux d'installation de la MDB

Lors de l'installation d'une MDB Microsoft SQL Server sur un ordinateur exécutant Windows, les fichiers journaux sont stockés aux emplacements suivants :

- %TEMP%\ITRM\database\setup.log
- %TEMP%\ITRM\database\mdb_install\install_*xxxx*.log
- *répertoire_installation_Client Automation*\database\setup.log

Lors de l'installation d'une MDB Oracle sur un ordinateur exécutant Sun Solaris, les fichiers journaux sont stockés aux emplacements suivants :

- /tmp/CAInstaller.ca-cms-mdb-schema.install.log
- *répertoire_installation_Client Automation*/database/setup.log
- *répertoire_installation_Client Automation*/database/mdb_install/install_*xxxx*.log

Sous Solaris, certains fichiers journaux se trouvent également dans :

- *répertoire_installation_Client Automation*/log/mdbinstall.log
- *répertoire_installation_Client Automation*/log/mdbupgrade.log

  Si l'installation échoue rapidement, les fichiers journaux peuvent être conservés dans /tmp/mdbinstall.log.

Mises à niveau de la MDB

Cette version prend en charge les mises à niveau de MDB suivantes :

- Gestionnaire DSM 12.5 SP1 ou version ultérieure avec la MDB Microsoft SQL Server installée localement ou à distance
- Gestionnaire DSM 12.5 SP1 ou version ultérieure avec la MDB Oracle 11g installée à distance sur Solaris, Linux ou Windows
- Gestionnaire DSM patché et MDB Oracle installés localement ou à distance sur Windows, Linux et Solaris

  Remarque : Le serveur Oracle 10g doit d'abord être mis à niveau vers Oracle 11 g R2. De même, avant de lancer l'installation du gestionnaire DSM, mettez à niveau le client Oracle sur ce gestionnaire DSM.

Si le serveur de base de données est distant, la MDB est mise à niveau en même temps que le gestionnaire DSM avec la version actuelle. Pour Microsoft SQL Server, aucune interaction d'utilisateur n'est requise, car les détails de base de données sont récupérés à partir du magasin de configurations. Pour Oracle, définissez la variable d'environnement ORACLE_HOME et saisissez le nom de service Oracle, le nom TNS et les mots de passe mdbadmin et système.

Si des sessions de base de données existantes sont détectées lors de la mise à niveau, chacune d'elles sera affichée avec les noms de l'utilisateur de la base de données, l'ID du processus et l'ordinateur hôte. Les sessions de base de données figurent dans deux listes d'une boîte de dialogue. La première liste concerne les sessions qui doivent être fermées avant d'autoriser la poursuite de la mise à niveau. Cette liste inclut des sessions appartenant à des utilisateurs de la base de données membres de rôles créés par le schéma DSM. Les rôles représentatifs sont ams_group, ca_itrm_group, ca_itrm_group_ro (Oracle uniquement), ca_itrm_group_ams, upmuser_group et mdbadmin (Oracle uniquement). Des rôles CCS (pour Microsoft SQL Server uniquement), tels que emadmin, emuser, uniadmin, uniuser, wvadmin et wvuser sont également inclus dans la première liste. Les rôles sont lus à partir d'un fichier de configuration sur l'image du DVD.)

La deuxième liste contient toute session restante appartenant à d'autres utilisateurs de la base de données. Nous recommandons de fermer également ces sessions, mais cette étape n'est pas obligatoire. Vous pouvez continuer la mise à niveau en laissant ces sessions ouvertes.

Pour actualiser les listes à mesure que vous fermez des sessions de base de données ouvertes, utilisez Actualiser dans cette boîte de dialogue. Le bouton Continuer est activé uniquement si la première liste de sessions de base de données est vide.

Désinstallation

Client Automation ne prend pas en charge la désinstallation du schéma de la MDB. Pour supprimer des données spécifiques de la MDB, vous pouvez utiliser le script de désinstallation de données lors d'une désinstallation de gestionnaire DSM. Vous pouvez également utiliser la fonctionnalité de Microsoft SQL Server et Oracle pour supprimer et recréer des instances de la MDB.

Remarques spéciales sur les installations Client Automation

Voici quelques remarques et recommandations destinées aux utilisateurs expérimentés concernant des scénarios d'installation spéciaux.

Paramètres de stratégie de sécurité

Les stratégies de sécurité suivantes doivent être activées pour l'ouverture de session utilisateur utilisée pour l'installation du gestionnaire DSM ou de la base de données de gestion (MDB).

- Accès à cet ordinateur à partir du réseau
- Fonctionner comme une partie intégrante du système d'exploitation
- Autoriser l'ouverture de session via Terminal Services
- Se connecter en tant que service

Vous pouvez activer ces stratégies via le Panneau de configuration Windows, Outils d'administration, Stratégie de sécurité locale.

Redémarrage de CAM et de SSA PMUX

Que vous décidiez d'installer la connectivité du réseau étendu (ENC) ou non, le programme d'installation de Client Automation invoquera en interne Message Queuing (CAM) et le programme d'installation de Secure Socket Adapter Port Multiplexer (SSA PMUX), ce qui entraînera le redémarrage de CAM et de SSA PMUX si nécessaire.

Remarque : Le redémarrage de SSA PMUX s'applique uniquement à Windows.

Pour plus d'informations sur ENC, consultez le chapitre "Connectivité du réseau étendu (ENC)".

Disponibilité de l'inventaire logiciel

Après l'installation d'un gestionnaire de domaines, l'inventaire logiciel n'est pas complètement disponible, car les définitions de logiciels sont importées dans la MDB par une tâche de moteur qui doit, par défaut, s'exécuter à minuit.

Installation du gestionnaire DSM avec une MDB SQL Server distante via IPV6

Si vous installez le gestionnaire DSM (domaine ou entreprise) avec une MDB SQL Server distante via IPv6, procédez comme suit avant de lancer l'installation :

1. Sur l'ordinateur gestionnaire, définissez la valeur de la clé de registre suivante sur 1 :

   ```
   HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)
   ```

2. Vérifiez les points suivants :
   - Le nom d'hôte de l'ordinateur MDB correspond à une adresse IPv6 globale.
   - La recherche inversée de l'adresse IPv6 renvoie le même nom d'hôte MDB.
3. Assurez-vous que l'ordinateur MDB correspond à une seule adresse IPv6 sur l'ordinateur gestionnaire DSM utilisé pour atteindre l'ordinateur MDB.

   Cela signifie que vous devez supprimer les enregistrements IPv4 DNS pour l'ordinateur MDB sur les serveurs DNS que l'ordinateur gestionnaire utilise, ainsi que les enregistrements IPv6 DNS avec des adresses que l'ordinateur gestionnaire ne peut utiliser pour atteindre l'ordinateur MDB. Le cache DNS sur le gestionnaire DSM doit être vidé si nécessaire. Sinon, JDBC ne peut pas se connecter à la MDB, ce qui affecte ensuite l'installation des composants Java CCS, CIC et MDB.

Installation du gestionnaire de domaines à l'aide de la MDB SQL Server distante avec l'instance nommée

Pour installer correctement le gestionnaire de domaines à l'aide d'une MDB SQL Server distante avec une instance nommée, assurez-vous que le navigateur SQL Server est exécuté sur le système MDB distant. Avant de commencer l'installation, vérifiez que le gestionnaire de domaines peut se connecter à la MDB distante et que le navigateur SQL Microsoft fonctionne correctement en exécutant la commande suivante sur le gestionnaire de domaines :

```
sqlcmd -E -d mdb -S nom du serveur MDB [\nom de l'instance] -q "sélectionner * dans mdb"
```

Installation de l'agent Remote Control autonome

Vous pouvez configurer la fonction Remote Control (RC) de Client Automation en mode autonome. Dans ce mode, l'agent RC utilise des stratégies de sécurité et de configuration locales, plutôt que les stratégies envoyées par un gestionnaire de domaine central.

Le support d'installation de Client Automation (DVD) contient un assistant d'installation distinct, appelé setup_rc, pour installer un agent RC autonome.

L'installation de l'agent RC autonome active uniquement les modules d'extension CAF suivants :

- pmux
- rchost
- smserver

Setup_rc peut être trouvé sous :

- WindowsProductFiles_x86\AgentRC
- LinuxProductFiles_x86/rc_agent

Installation sur Solaris Intel

Avant de commencer l'installation de Client Automation sur la plate-forme Solaris (Intel), vérifiez que vous avez installé les patchs suivants pour le package SUNWlibC :

- 109148-07
- 108436-16

Ces patchs permettent d'installer des bibliothèques d'exécution C++ standard.

Pour vérifier la présence de ces patchs, utilisez la commande suivante :

```
showrev –p | grep SUNWlibC
```

Le résultat suivant apparaît :

```
Patch: 108436-16 Obsoletes: Requires: 109148-07 Incompatibles: Packages: SUNWlibC
```

Remarque : CA Client Automation dépend de CAPKI, qui dépend de libucb sur Solaris Intel. Sur Solaris intel 11, si libucb n'est pas installé par défaut, l'installation échoue.

Procédez comme suit pour installer libucb sur Solaris intel 11 :

1. Pour identifier le package, exécutez la commande suivante :

   pkg search -r /usr/ucblib/libucb.so.1

2. Pour installer le package, exécutez la commande suivante :

   pkg install <nom_package>

Variable d'environnement PATH pour Solaris Intel

Le démarrage du shell appelle les scripts de démarrage. Notez que les shells sh (comme Bash) appelle /etc/profile, puis ~/.profile. Toutefois, dans Solaris 11 Intel, ~/.profile pour l'utilisateur root remplace la variable d'environnement PATH.

Lorsque la variable PATH ne contient aucun chemin d'accès CA, vérifiez que vous utilisez le script de démarrage en tant que source de la manière suivante :

- . /etc/profile.CA tout ou
- source /etc/csh_login.CA all

Accès au service Web de VMware ESX

Pour accéder au service Web de VMware ESX, vous devez fournir les informations d'identification de connexion suivantes pour l'utilisateur d'un ordinateur hôte VMware ESX :

Nom d'hôte

Nom de l'hôte ESX pour lequel l'inventaire de gestion des actifs doit être collecté (possibilité d'indiquer une adresse IP)

Nom d'utilisateur du service Web

Nom d'un utilisateur de VMware ESX qui a le rôle Administrateur ou Lecture seule au niveau du système VMware

Mot de passe du service Web

Mot de passe de l'utilisateur de VMware ESX spécifié

URL du service Web

URL du service Web, sous la forme suivante :

`https://ESXHostFQDNservername/sdk`

ESXHostFQDNservername correspond au nom d'hôte complet du serveur ESX. Vous pouvez également entrer une adresse IP.

La collecte d'inventaires ESX a lieu à l'aide du moteur du service Web (SOAP). Par défaut, le service Web s'exécute sur le port 443 en tant que service Web sécurisé acccessible via le protocole SSL sur HTTPS.

Installation du composant Remote Control sous Linux

La fonction Remote Control (RC) de Client Automation prend en charge Linux. Cet environnement d'exploitation prend uniquement en charge le composant hôte RC.

Si l'agent RC autonome est requis dans cet environnement d'exploitation, il doit être installé à partir du répertoire LinuxProductFiles_x86/rc_agent.

Les agents autonomes ne peuvent pas être déployés à l'aide du programme d'installation Software Delivery ou interactive.

Installation du composant Remote Control sur Apple Mac OS X

La fonction Remote Control (RC) de Client Automation prend en charge Apple Mac OS X. Cet environnement d'exploitation prend uniquement en charge le composant hôte Remote Control.

Le mode de contrôle sécurisé n'est pas pris en charge. Tous les autres modes de contrôle sont pris en charge (Vue furtive, Affichage, Partagé, Classe et Exclusif).

Comme avec Linux, les options de la visionneuse pour désactiver le papier peint de l'hôte et d'autres caractéristiques 'expérience utilisateur' n'ont aucun effet.

Important : Après avoir installé, ré-installé, réparé ou mis à niveau un agent Remote Control sur une plate-forme Mac OS X, CA recommande de se déconnecter du système et de se reconnecter. Cela garantit que les processus DSM essentiels sont démarrés dans le bon contexte de l'utilisateur. Si cette étape est omise, les tentatives de connexion de Remote control seront rejetées avec le message suivant : "L'hôte n'a pas pu ouvrir le bureau de l'utilisateur actuel."

Accès au partage pour le serveur de démarrage

Le serveur de démarrage est toujours installé dans un serveur de modularité et ses détails de configuration sont spécifiés sur les pages de configuration du serveur de modularité de l'assistant d'installation.

Si vous souhaitez utiliser l'accès au partage au lieu de TFTP (paramètre par défaut), cliquez sur le bouton Serveur de démarrage situé dans la zone Configuration avancée du serveur de la page Configurer le serveur de modularité, puis cochez la case "Activer l'utilisation des partages réseau Windows". Le programme d'installation crée des partages réseau en lecture seule, accessibles via le protocole SMB.

Pour plus d'informations sur le passage de TFTP à l'accès au partage et la désactivation du serveur PXE, consultez le *Manuel d'administration du système de gestion des installations de systèmes d'exploitation* faisant partie de la documentation en ligne de CA Client Automation (Bibliothèque).

Connexion du contrôleur de domaine lors de l'installation de CCS

Si la connexion au contrôleur de domaine est perdue lors de l'installation de CCS en tant qu'administrateur de domaine, l'installation de CCS échouera lors de la tentative de validation des droits d'installation pour l'utilisateur, parfois avec un code de retour 1073741819.

Pour résoudre cela, rétablissez la connexion au contrôleur de domaine ou exécutez l'installation en tant qu'administrateur local.

Déplacement d'agent et de serveurs de modularité

Un agent est configuré pour se connecter à un seul gestionnaire de domaine à tout moment. Toutefois, l'agent peut être de nouveau configuré. Le déplacement d'un agent peut être déclenché par la commande suivante :

```
caf setserveraddress nouveau_serveur_modularité
```

Le déplacement d'un serveur de modularité peut être déclenché par la commande suivante :

```
cserver config -h nouveau_gestionnaire_domaine
cserver register
```

Dès qu'un calendrier est mis à jour sur un serveur CA Common Services (CCS) (situé sur un gestionnaire DSM), les agents CCS (situés sur des serveurs de modularité DSM) doivent être mis à jour. Exécutez la procédure du serveur de modularité "Synchroniser le calendrier CCS" sur chaque serveur de modularité situé en aval avec l'agent CCS installé.

Si vous déplacez un serveur de modularité d'un gestionnaire à un autre, à l'aide de la commande cserver config -h nouveau_gestionnaire, l'agent CCS (situé sur ce serveur de modularité) est automatiquement reconfiguré pour se connecter au nouveau gestionnaire.

Remarque : Pour assurer la conservation des valeurs CCS lors du réenregistrement du serveur, remplacez l'option -h par -i au niveau de la commande cserver.

Toutefois, si le serveur est déplacé à l'aide d'une stratégie, vous devez le reconfigurer manuellement ; dans le cas contraire, l'agent continuera à se connecter à l'ancien serveur CCS. Pour passer au serveur CCS sur le nouveau_gestionnaire, utilisez les commandes suivantes sur l'ordinateur du serveur de modularité :

```
cautenv setlocal CA_CALENDAR_NODE nouvelle_adresse_gestionnaire
cautenv setlocal CA_OPR_PROXY nouvelle_adresse_gestionnaire
unicntrl stop all
unicntrl start all
```

Gestionnaire DSM avec gestionnaire WorldView CCS ou CCS y compris MDB sur un contrôleur de domaine

Dans ce scénario d'installation (gestionnaire DSM avec gestionnaire WorldView CA Common Services (CCS) ou CCS y compris MDB sur un contrôleur de domaine), la restriction CCS suivante s'applique :

Le gestionnaire CCS WorldView ne peut pas être installé sur un serveur désigné comme un contrôleur de domaine.

Ceci est dû à la sécurité IPSEC, qui écrase les privilèges de l'utilisateur pour le serveur COM Microsoft pendant le démarrage de l'objet COM de propagation de sévérité CA.

Cette restriction empêche CA Client Automation d'installer le gestionnaire WorldView CCS sur un contrôleur de domaine. Le gestionnaire DSM et les installations "CCS y compris MDB" sont concernés. Pour installer correctement le gestionnaire DSM, vous disposez des options suivantes sur un contrôleur de domaine :

- Désactiver CCS (aucune fonctionnalité de CCS n'est disponible).
- Installer MDB et CCS à distance (le gestionnaire WorldView CCS est installé côté MDB).

Installation du serveur de modularité sous Linux

Lors de l'installation d'un serveur de modularité sous Linux à l'aide de DMDeploy ou de Software Delivery avec le package en anglais (ENU) du serveur de modularité CA DSM Linux (Intel), le logiciel CA Common Services n'est *pas* installé. Lorsque CCS est requis avec un serveur de modularité sous Linux, il doit être installé de manière interactive à partir du DVD.

Installation et enregistrement des composants UNIX et Mac OS X

Ces composants ne sont pas enregistrés automatiquement dans les bibliothèques de livraison de logiciels et de déploiement de l'infrastructure lors de leur installation sur un gestionnaire de domaines.

Pour mettre à disposition ces packages sur un gestionnaire de domaine, vous devez les importer à l'aide de l'outil dsmPush ou du CD vers la bibliothèque de packages logiciels et la zone de packages logiciels de déploiement de l'infrastructure du gestionnaire (fichier dsmPush.dms dans le répertoire racine du DVD).

Entrez la commande suivante :

```
dmscript dsmPush.dms copy -I emplacement_image_CD
```

Pour enregistrer ces packages dans la bibliothèque de packages logiciels, vous pouvez également les copier et coller à partir du CD approprié vers le dossier correspondant à la bibliothèque de packages logiciels dans l'explorateur DSM.

Remarques concernant l'agent UNIX

Les environnements d'exploitation UNIX actuellement pris en charge par l'agent UNIX dans Client Automation sont répertoriés dans la matrice de compatibilité disponible dans la bibliothèque Client Automation ou sur le site du support de CA. Les plates-formes qui y figurent sont également celles sur lesquelles l'outil de packaging pour Linux et UNIX fonctionne.

Installation des conditions préalables pour l'agent sous Sun Solaris

Avant d'installer l'agent UNIX sur un ordinateur Sun Solaris, vous devez vous assurer que les paramètres de configuration kernel minimaux requis sont définis.

Pour définir ou modifier les paramètres de configuration kernel pour Solaris 5.10

Pour Solaris 5.10, le paramètre de configuration de contrôle des ressources max-shm-memory doit être défini sur 5242880.

ou pour des versions ultérieures et paramètre max-sem-ids doit être défini sur 256 ou plus.

1. Recherchez les valeurs actuelles de ces paramètres à l'aide de la commande prctl, par exemple :

   ```
   prctl –P –n project.max-shm-memory –i project user.root
   ```

   ```
   prctl –P –n project.max-sem-ids –i project user.root
   ```

2. Si les paramètres de configuration du contrôle des ressources doivent être mis à jour, utilisez *l'une* des commandes suivantes :

   - Utilisez prctl pour modifier les paramètres de configuration de contrôle des ressources, par exemple :

     ```
     prctl -n project.max-shm-memory -v 5242880 -r -i project user.root
     ```

     ```
     prctl -n project.max-sem-ids -v 256 -r -i project user.root
     ```

     Remarque : Les paramètres de configuration modifiés à l'aide de la commande prctl ne sont *pas* permanents. Vous devez exécuter à nouveau les commandes après le redémarrage du système.

   - Utilisez projmod pour modifier les paramètres de configuration de contrôle des ressources, par exemple :

     ```
     projmod -s -K "project.max-shm-memory=(priv,5242880,deny)" user.root
     ```

     ```
     projmod -s -K "project.max-sem-ids=(priv,256,deny)" user.root
     ```

     Remarque : Les paramètres de configuration modifiés à l'aide de la commande projmod sont permanents après le redémarrage du système.

Installation des conditions préalables pour l'agent sous IBM AIX

Lorsque vous installez l'agent UNIX Client Automation sur un ordinateur IBM AIX fonctionnant avec la version 5.3 ou ultérieure d'AIX, les dernières bibliothèques de l'environnement d'exécution d'IBM sont installées.

Téléchargement de Software Delivery et agents UNIX

Les observations suivantes s'appliquent lorsque la méthode de téléchargement de Software Delivery est définie sur la méthode Interne NOS.

Le kernel Sun Solaris ne prend pas en charge le montage de partages Samba.

Si le serveur de modularité possède des points de montage NFS configurés uniquement (s'il n'utilise pas Samba, en d'autres termes), les agents Sun Solaris utilisent alors automatiquement NFS.

Si le serveur de modularité dispose de partages Samba configurés, tandis que le paramètre NOSLessSwitchAllowed possède la valeur 1 (True (Vrai)), les agents Sun Solaris reviennent alors à l'utilisation de la méthode de téléchargement Interne sans serveur NOS (Network Object Server).

Si le serveur de modularité dispose de partages Samba configurés, tandis que le paramètre NOSLessSwitchAllowed possède la valeur 0 (False (Faux)), le téléchargement échoue, même si le serveur de modularité possède aussi des points de montage NFS configurés.

La valeur actuelle du paramètre NOSLessSwitchAllowed peut être vérifiée en exécutant la commande suivante :

```
ccnfcmda -cmd GetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed
```

La valeur du paramètre NOSLessSwitchAllowed peut être définie par 1 en exécutant la commande suivante :

```
ccnfcmda -cmd SetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed -v 1
```

Remarque : Pour plus d'informations sur la commande ccnfcmda de l'agent de configuration, saisissez <command> / ? dans l'invite de commande.

Remarque concernant l'installation du service de transport de données

Sous Windows, la fonction de service de transport de données (DTS) n'est pas intégrée dans le module d'extension de l'agent Software Delivery (SD), mais dans un package d'installation séparé. Cela signifie que si vous souhaitez utiliser la fonction DTS, par exemple, pour employer la méthode de téléchargement DTS pour un agent spécifique, vous devez déployer le package d'installation DTS distinct vers cet agent.

Sous Linux ou UNIX, la fonction de service de transport de données est incluse dans le module d'extension Software Delivery (SD). En d'autres termes, DTS est installé avec le package d'installation de l'agent SD.

Attribution de nouveaux noms aux serveurs de gestionnaires et de modularité

CA Client Automation (Client Automation) prend en charge l'attribution de nouveaux noms aux gestionnaires d'entreprise et de domaines via l'explorateur DSM à l'aide des boîtes de dialogue Propriétés de l'entreprise ou Propriétés du domaine. Les champs Nom, Coordonnées et Description peuvent être modifiés et leurs valeurs sont répliquées entre les gestionnaires d'entreprise et de domaines.

Client Automation ne prend pas en charge l'attribution de nouveaux noms aux serveurs de modularité.

Noms de systèmes en tant que noms de domaines complets

Chaque fois que le programme d'installation Client Automation requiert la saisie d'un nom de système, nous vous recommandons vivement de saisir un nom de domaine complet (FQDN) incluant un suffixe afin de pouvoir atteindre les systèmes informatiques d'autres domaines de réseau, même si la transmission de la requête n'est pas configurée pour tous les DNS impliqués.

Installation de Client Automation lorsque Unicenter NSM r11 est préinstallé

Si Unicenter NSM r11 est installé avant CA Client Automation, Unicenter NSM doit installer les composants CCS suivants avant de commencer l'installation de CA Client Automation :

Composants Unicenter NSM :

- Management Database
  - MDB pour Microsoft SQL Server
- WorldView
  - Client administratif
  - Gestionnaire WorldView
- Gestion Enterprise
  - Client administratif
  - Gestion des événements
    - Agent d'événements
    - Gestionnaire d'événements
- Détection continue
  - Agent de détection continue
  - Gestionnaire de détection continue

Lancez l'installation de Unicenter NSM, vérifiez si tous les composants répertoriés sont installés et installez les composants manquants.

Une fois l'installation de Unicenter NSM terminée, vous pouvez installer CA Client Automation.

Spécifier le numéro de port pour la console Web pendant l'installation

La modification de la clé SQLServer.PortNo avec le numéro de port de la base de données dans le fichier wacconfig.properties n'est plus valide avec le support multi-gestionnaires de la console Web. Le numéro de port correct doit être fourni pendant l'installation et ne peut pas être modifié ultérieurement.

Remarque concernant l'ajout de la console Web via l'option de modification de l'installation

Si vous envisagez d'ajouter la console Web à l'aide de la méthode de modification de l'installation, vous devez vous assurer que l'espace disque disponible est de 8 Go minimum !

Désactivation de l'antivirus durant l'installation et la désinstallation

Nous vous recommandons de désactiver le logiciel antivirus avant de démarrer l'installation ou la désinstallation de CA Client Automation. Si un logiciel antivirus est activé, des interférences peuvent se produire au cours du processus d'installation ou de désinstallation.

Désactivation du service Serveur de secteur à distance durant l'installation

Si un service RSS (Serveur de secteur à distance) provenant d'une version antérieure Unicenter Asset Management est installé sur l'ordinateur sur lequel vous allez installer Client Automation, vous devez l'arrêter avant de démarrer l'installation de Client Automation. Le service RSS doit être désactivé avant qu'il n'essaie de redémarrer automatiquement.

Désactivez le service Serveur de secteur Asset Management du Gestionnaire de contrôle des services. Une fois l'installation terminée, réactivez le service.

Accès : partage réseau Windows XP et modèle de sécurité pour les comptes locaux

Si cette stratégie Windows XP est définie sur Invité seulement, quiconque essayant de s'authentifier en tant qu'utilisateur local est mappé au compte Invité, qui est désactivé par défaut. Un échec de l'authentification s'ensuit.

Pour remédier à ce problème, consultez la documentation de Microsoft à l'adresse suivante :

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/506.mspx

Observations sur Windows Server 2003

Sur les serveurs Windows NT et Windows 2000, les accès anonymes, également appelés sessions NULL, pouvaient être utilisés par défaut pour accéder aux ressources du réseau. Des partages de système de fichiers, appelés partages de session NULL, pouvaient être configurés pour accepter des sessions NULL. Cette méthode a toujours été privilégiée pour permettre à des agents Software Delivery (SD) exécutés sous le compte LocalSystem d'accéder à la bibliothèque de packages logiciels (partage SDLIBRARY$) sur le serveur de modularité.

Avec Windows Server 2003, Microsoft accroît le niveau de sécurité par rapport aux versions précédentes du système d'exploitation du serveur. Par défaut, l'accès anonyme et les partages de session NULL sont désactivés. Le besoin d'un accès anonyme a été éliminé pour les ordinateurs appartenant au domaine, en transformant les comptes de domaine de l'ordinateur en véritables entités du système de sécurité Windows. Dans les domaines Windows 2000 et ultérieurement dans les domaines Windows Server 2003, des droits d'accès peuvent être accordés à la fois à des comptes d'ordinateur et d'utilisateur.

Sous Windows Server 2003, les partages de session NULL ne sont pas utilisés pour l'accès de ces agents à la bibliothèque de packages logiciels. En fait, SD considère que les agents ont accès à la bibliothèque via leurs comptes de domaine d'ordinateur. Bien que plus sécurisée et conforme aux recommandations de Microsoft, cette approche ne constitue pas une solution complète pour tous les environnements d'exploitation d'agent SD pris en charge.

Pour en savoir plus sur l'évolution de l'accès anonyme dans les environnements d'exploitation Windows, veuillez consulter l'article 278259 de la base de connaissances de l'assistance Microsoft.

Installations administratives de MSI avec SDMSILIB sous Windows Server 2003

Lorsque vous effectuez des installations administratives de MSI pour déployer des packages vers le partage SDMSILIB, la méthode sd_sscmd libraryaccess ne suffit pas pour se connecter à ce partage. Les agents doivent pouvoir accéder à ce partage, même si des installations ou des configurations utilisant la fonction Software Delivery (SD) ne sont pas exécutées. En effet, les demandes d'accès au partage SDMSILIB peuvent à tout moment être effectuées par des installations MSI, par exemple, lors d'une réparation ou de la mise en place de mécanismes d'autorétablissement. En fait, SD considère que les agents ont accès au partage SDMSILIB via leurs comptes de domaine d'ordinateur.

Accès à la bibliothèque MSI Windows 2003 SP1 : Restriction de l'accès anonyme aux canaux et partages nommés

Par défaut, l'accès anonyme aux partages réseau sous Windows 2003 Service Pack 1 est refusé.

Pour des installations en réseau des packages MSI à partir du partage SDMSILIB ou de l'accès anonyme au partage SDLIBRARY$ sur un ordinateur exécutant Windows 2003 Service Pack 1, vous devez effectuer les opérations suivantes :

- Définissez l'option de sécurité suivante dans la stratégie de sécurité locale : "Accès réseau : Restreindre l'accès anonyme aux canaux et partages nommés – Désactivé"
- Redémarrez le système pour valider les modifications.

Connexion des agents SD aux serveurs de modularité SD

Les stratégies suivantes s'appliquent uniquement lorsque des agents Software Delivery (SD) sont connectés à des serveurs de modularité SD exécutant Windows Server 2003, et lorsque la stratégie de sécurité locale "Accès réseau : Restreindre l'accès anonyme aux canaux et partages nommés" est définie sur Activé sur le gestionnaire ou le serveur de modularité.

Les agents SD exécutés sur des ordinateurs Windows XP ou Windows Server 2003, qui n'appartiennent à aucun domaine ou qui appartiennent à un domaine non approuvé autre que le gestionnaire SD sur lequel réside le partage de la bibliothèque de packages logiciels, se voient également refuser l'accès.

Pour résoudre les problèmes d'accès des agents SD sous Windows XP ou Windows Server 2003, vous pouvez créer manuellement un compte utilisateur dédié sur le serveur de modularité et l'ajouter au groupe Tout le monde. Un accès en lecture seule aux partages SDLIBRARY$ vous sera alors accordé. Le nom et le mot de passe de l'utilisateur doivent être saisis dans l'espace de stockage de configuration commun de chaque gestionnaire de domaines et serveur de modularité exécuté sur la nouvelle plate-forme de gestionnaire Windows.

Afin d'éviter les échecs, les agents SD optent automatiquement pour un téléchargement interne non-NOS, en cas de refus d'accès à la bibliothèque. Ce comportement peur être désactivé en définissant le paramètre NOSLessSwitchAllowed sur False dans la section itrm/usd/agent de la stratégie de configuration.

Environnements d'exploitation Windows Server 2008 Core

Cette section décrit les problèmes connus et les solutions à appliquer aux systèmes d'exploitation Windows Server 2008 Server Core.

Dépendance avec l'interface utilisateur graphique (IUG)

Le serveur principal pour Windows Server 2008 fournit des fonctionnalités IUG limitées. En raison de la dépendance avec l'interface utilisateur graphique, les options suivantes de l'agent Client Automation ne sont pas prises en charge :

- Discussion instantanée Remote Control
- visionneuse Remote Control
- Catalogue de logiciels
- SysTray

Dépendance avec IE

Le serveur principal Windows Server 2008 ne prend pas en charge les programmes d'installation utilisant le format HTML, car ils dépendent d'Internet Explorer.

Pour installer les agents Client Automation, utilisez *une* des procédures suivantes :

- Lancez le média d'installation, accédez au répertoire WindowsProductFiles et exécutez le fichier setup.exe.
- A partir de l'explorateur DSM, utilisez DMDeploy pour déployer les modules d'extension de l'agent.

Désinstallation des agents

Le serveur principal pour Windows Server 2008 ne prend pas en charge la fonction Ajouter ou supprimer des programmes. Pour désinstaller les agents, vous devez exécuter l'outil msiexec à partir de la ligne de commande.

Pour plus d'informations sur msiexec, consultez la section Outil d'installation msiexec (page 181).

Options non prises en charge

Le serveur principal de Windows Server 2008 ne prend pas en charge les éléments suivants :

- Aide en ligne des agents
- Mode d'opération "Forcer la déconnexion de l'utilisateur avant l'exécution du job" pour le bouclier de connexion
- L'option de déconnexion des options de procédure "Niveau de redémarrage avant exécution" et "Niveau de redémarrage après exécution"

Remarques concernant le pare-feu et les ports

Certains systèmes d'exploitation, tels que Windows XP et Red Hat, incluent une fonction de pare-feu pouvant empêcher l'établissement de connexions à distance. Parmi ces dernières, on distingue les connexions d'autres composants DSM, tels que des serveurs de modularité. Pour que CA Client Automation puisse fonctionner correctement, il sera peut-être nécessaire de reconfigurer le pare-feu.

Vous trouverez une présentation des ports actuellement utilisés par CA Client Automation et ses composants individuels dans l'annexe "Ports utilisés par CA Client Automation" (page 553).

Bibliothèques de compatibilité pour Linux

Le programme d'installation DSM part du principe que certaines bibliothèques dépendantes existent dans le système. Si ce n'est pas le cas, les composants installés ne fonctionneront peut-être pas correctement.

Le tableau ci-dessous détaille les conditions requises pour la bibliothèque de logiciels. Ces bibliothèques doivent être présentes sur les hôtes Linux avant d'installer des composants DSM.

Distribution/version de Linux	Packages RPM requis
Red Hat 5 Enterprise Linux	glibc 2.3.3-84 compat-libstdc++ 33-3.2,3-61 Pour les versions 64 Bits du SE : ncurses 5.4-1.3 (i386) ou ncurses-devel 5.4-13 (i386) zlib 1.1.4-8.1 (i386) ou zlib-devel 1.2.1.2-1.2 (i386)
SuSE Linux Enterprise Server 10	glibc 2.3.3-84 compat 2004.4.2-3 libstdc++ 3.2.2-38

Remarque : Pour connaître les dernières informations sur les bibliothèques de compatibilité et les packages système supplémentaires requis, consultez le site Web de l'assistance technique de votre fournisseur Linux.

Conditions préalables requises de MSI pour le programme d'installation

Dans tous les environnements d'exploitation Windows, le programme d'installation Client Automation requiert le moteur Microsoft Windows Installer (MSI) 2.0. Si cette version n'est pas disponible, l'assistant d'installation l'ajoute automatiquement avant toute étape d'installation. Pour la mise à niveau vers MSI 2.0, il n'est pas nécessaire de redémarrer le système,

Sous Windows 2003, il est peu probable que des redémarrages se produisent, car MSI 2.0 a normalement été installé avec le système d'exploitation.

Composant	Plate-forme Windows à installer	Version MSI attendue	Action effectuée par le programme d'installation si la version attendue de MSI n'est pas présente sur l'ordinateur cible
IU	Tous	2.0	Installation/Mise à niveau vers la version 2.0
Gestionnaire	Tous	2.0	Installation/Mise à niveau vers la version 2.0
Serveur	Tous	2.0	Installation/Mise à niveau vers la version 2.0
Agent	2003	2.0	Installation/Mise à niveau vers la version 2.0

Remarque : Si des agents ont été installés à l'aide de la fonction Software Delivery ou Déploiement de l'infrastructure, vous devez vérifier que Microsoft Windows Installer est déjà installé sur les ordinateurs cibles. Si nécessaire, vous pouvez télécharger Microsoft Windows Installer à partir du site Web Microsoft (www.microsoft.com).

Partage de la MDB entre CA Service Desk Manager et Client Automation

Si vous envisagez de partager la même MDB entre CA Service Desk Manager et Client Automation, vous devez d'abord installer CA Service Desk Manager, puis Client Automation.

Installation administrative sous Windows

Cette option d'installation manuelle ne concerne que les environnements d'exploitation Windows. Une installation administrative permet à la fonction Microsoft Windows Installer de décompresser le contenu de l'image d'installation et de copier cette dernière dans un partage réseau.

Répertoires d'installation sous Windows

La structure des répertoires d'installation dans les environnements Windows, ainsi que les règles et restrictions s'y appliquant, sont décrites ci-dessous :

Chemin de base par défaut

`C:\Program Files\CA\DSM`

Vous pouvez modifier ce chemin lorsque vous y êtes invité.

Chemin d'accès aux composants partagés

Les composants partagés sont installés dans différents répertoires. Par défaut, Windows Installer crée des répertoires pour chacun des composants partagés dans le chemin de base suivant :

`C:\Program Files\CA\SC`

Vous pouvez modifier ce chemin lorsque vous y êtes invité.

Variable d'environnement PATH

Durant l'installation, la variable d'environnement PATH est étendue à

basepath\bin

Cependant, dans le cas suivant, la variable d'environnement PATH peut ne pas être automatiquement mise à jour lors de l'installation :

Lorsque vous effectuez l'installation via une session de Terminal Server, la modification de la variable PATH n'est validée qu'après avoir effectué l'une des opérations suivantes :

- Déconnexion et reconnexion au système
- Redémarrez le système

Ce comportement est causé par le système d'exploitation Microsoft et ne peut donc pas être modifié.

Par conséquent, dans certains systèmes Windows, vous ne pouvez pas utiliser l'interface de ligne de commande CAF (Common Application Framework) tant que les modifications de la variable PATH n'ont pas été validées.

La longueur maximale de la variable PATH est déterminée par l'environnement d'exploitation Windows utilisé. Au cours de l'installation, la longueur réelle de la variable PATH est vérifiée. Si la longueur ne vous permet pas d'ajouter des noms de répertoire supplémentaires, le processus d'installation est interrompu.

Répertoires d'installation sous Linux et UNIX

La structure des répertoires d'installation de Client Automation dans les environnements Linux et UNIX , ainsi que les règles et restrictions s'y appliquant, sont décrites ci-dessous :

Chemin de base par défaut

Le répertoire d'installation par défaut de Client Automation est :

```
/opt/CA/DSM
```

Le répertoire d'installation de Client Automation est également référencé par la variable d'environnement $CA_ITRM_BASEDIR.

Vous pouvez modifier ce chemin lorsque vous y êtes invité.

Chemin d'accès aux composants partagés

Les composants partagés sont installés dans différents répertoires. Par défaut, le programme d'installation crée des répertoires pour chacun des composants partagés dans le chemin de base suivant :

```
/opt/CA/SharedComponents
```

L'emplacement des composants communs est également référencé par la variable d'environnement $CASHCOMP, qui est configurée par le programme d'installation.

Remarque : $CASHCOMP est partagé par tous les produits CA sur un ordinateur. Si cette valeur a été définie (en installant précédemment un autre produit CA), il est alors impossible de la modifier dans l'installation de Client Automation. Le programme d'installation sera limité aux paramètres existants.

Variable d'environnement PATH

Vous pouvez déterminer si vous souhaitez ou non mettre la variable d'environnement PATH à jour dans l'ensemble du système à la fin de l'installation. Si vous ne le faites pas, vous pouvez toujours configurer le chemin manuellement après l'installation, ainsi que d'autres variables d'environnement requises pour un fonctionnement correct de Client Automation. Pour effectuer cette opération dans un shell Bourne/Korn/bash, exécutez la commande suivante :

```
N°. $CA_ITRM_BASEDIR/scripts/dsmenv
```

Pour configurer l'environnement dans le shell C, exécutez la commande suivante :

```
# source $CA_ITRM_BASEDIR/scripts/dsmenvcsh
```

Installation de collecteur d'alertes

Vous pouvez définir le rôle sous lequel le collecteur d'alertes est exécuté lors du déploiement. Configurez le collecteur d'alertes dans l'un des rôles suivants :

Conserver les alertes dans la MDB

Configure le collecteur d'alertes pour conserver les alertes dans la MDB.

Conserver les alertes dans la MDB et appliquer les actions configurées

Configure le collecteur pour conserver les alertes dans la MDB et effectuer les actions configurées, telles que l'envoi de courriels, le déclenchement d'interruptions SNMP ou l'écriture dans le journal d'événements Windows/CCS.

Conserver les alertes, appliquer les actions et transférer

Configure le collecteur pour conserver les alertes dans la MDB, effectuer les actions configurées et envoyer les alertes à un autre collecteur d'alertes.

Transférer

Configure le collecteur pour envoyer les alertes à un autre collecteur d'alertes.

Installez le collecteur d'alertes sur le gestionnaire d'entreprise, sur le gestionnaire de domaines ou sur un ordinateur autonome qui se connecte au gestionnaire de MDB sur le gestionnaire de domaines/d'entreprise. Vous pouvez également l'installer sur un ordinateur autonome sous le rôle *Transférer des alertes*.

La section suivante explique les rôles que vous pouvez sélectionner selon les configurations :

Sur le gestionnaire d'entreprise ou le serveur autonome se connectant à celui-ci :

Sélectionnez *Conserver les alertes dans la MDB.* Pour le gestionnaire d'entreprise, les autres rôles ne sont pas pris en charge.

Sur le gestionnaire de domaines ou le serveur autonome se connectant à celui-ci :

Sélectionnez *Conserver les alertes dans la MDB et appliquer les actions configurées* ou *Conserver les alertes dans la MDB, appliquer les actions configurées avant de les transférer.* Sélectionnez le dernier rôle lorsque le gestionnaire de domaines est lié à un gestionnaire d'entreprise pour envoyer des alertes à ce dernier. Sélectionnez d'autres rôles lorsque vous devez conserver les alertes dans la MDB ou les envoyer au collecteur d'alertes sur le gestionnaire d'entreprise.

Serveur Autonome : aucune connexion au gestionnaire de domaines ou d'entreprise

Sélectionnez *Transférer des alertes* pour envoyer des alertes à un autre collecteur d'alertes. Par exemple, dans un environnement ENC, installez le collecteur d'alertes sur le serveur ENC qui réside dans la zone DMZ pour que les alertes soient envoyées au collecteur d'alertes sur le gestionnaire de domaines.

Par défaut, vous pouvez installer le collecteur d'alertes directement sur le gestionnaire de domaines, le gestionnaire d'entreprise (le cas échéant) ou sur des serveurs distincts reliés aux MDB sur les gestionnaires. Pour gérer la charge croissante, procédez comme suit :

- Ajoutez des serveurs de collecteur d'alertes supplémentaires, chacun renvoyant au collecteur d'alertes sur le gestionnaire de domaines.
- Augmentez le nombre de processus de travail pour le pool d'applications DSM_WebService_HM sur IIS.

Restrictions concernant les noms d'ordinateurs, d'utilisateurs et de répertoires

Les noms d'ordinateurs, d'utilisateurs et de répertoires doivent être valides pour le système d'exploitation sur lequel est installé Client Automation et doivent respecter les restrictions imposées dans les sections suivantes :

- Restrictions concernant les noms d'ordinateurs (page 171)
- Restrictions concernant les noms d'utilisateurs (page 172)
- Restrictions concernant les noms de répertoires (page 172)

Restrictions concernant les noms d'ordinateurs

Les noms d'ordinateur doivent contenir les caractères ASCII suivants uniquement :

- alphanumérique
- tiret -

Les noms d'ordinateur ne doivent pas commencer par un tiret.

Important : Pour prendre en charge des noms d'hôtes localisés, cela signifie, des noms d'hôtes qui sont en langues locales autres que l'anglais américain (non-ENU), il faut que l'infrastructure sous-jacente du DNS (système de nom des domaines) prenne en charge le codage à caractères UTF-8 dans le DNS.

Restrictions concernant les noms d'utilisateurs

Les noms d'utilisateur doivent contenir les caractères ASCII suivants uniquement :

- alphanumérique
- arobase @
- dièse #
- dollar $
- trait de soulignement _

Les noms d'utilisateur ne doivent pas commencer par @, #, $ ou un chiffre.

Restrictions concernant les noms de répertoires

Un nom de répertoire doit commencer soit par :

- une lettre ASCII, a à z et A à Z, soit par
- un chiffre compris entre 0 et 9
- un trait de soulignement _

Il peut se poursuivre par :

- des lettres ASCII
- des chiffres
- tiret -
- trait de soulignement _
- point .
- tilde ~

En général, CA Technologies recommande de ne pas différentier les noms de chemin en fonction de la casse.

Remarques spécifiques à Windows :

- Les noms de répertoire absolus doivent commencer par une indication de lecteur (une lettre de lecteur immédiatement suivie de deux points), suivie d'une barre oblique inverse \, puis d'un chemin de répertoire relatif. Les chemins UNC ne sont pas autorisés.
- Les parenthèses (et) peuvent être utilisées après le premier caractère d'un nom de répertoire, mais lors de l'installation d'un gestionnaire, ces parenthèses (et), ainsi que le tiret - ne sont pas autorisés dans le nom de répertoire.
- Les espaces sont autorisés après le premier caractère d'un nom de répertoire.
- Les lettres majuscules ne se distinguent pas des minuscules (ainsi, a équivaut à A).
- Sous Windows, il n'est pas possible d'installer un gestionnaire avec une MDB distante ou locale à l'aide d'un nom de chemin UNC pour l'emplacement de l'image. Si l'emplacement de l'image se trouve sur un système distant, il doit être rendu accessible en tant que partage Windows. En outre, le nom du chemin ne doit pas contenir @.

Remarques spécifiques à Linux et à UNIX :

- Les chemins de répertoire absolus doivent commencer par une barre oblique /, suivie d'un chemin de répertoire relatif. Un chemin de répertoire relatif contient un certain nombre de noms de répertoire séparés par des barres obliques.
- Les lettres majuscules se distinguent des minuscules (ainsi, a est différent d'A).
- L'espace (les caractères d'espace et de tabulation, par exemple) n'est pas autorisé dans les chemins de répertoire d'installation.

Installation interactive à l'aide de l'assistant d'installation

L'assistant d'installation de Client Automation gère l'installation complète de tous les composants logiciels et de certaines conditions préalables requises. Si l'une de ces conditions n'est pas satisfaite, le programme d'installation affiche des messages d'erreur.

Vérification de l'espace disque avant l'installation

Le programme d'installation évalue la quantité d'espace disque requise pour installer les composants sélectionnés. L'installation se poursuit uniquement si l'espace disque disponible est suffisant.

Cependant, des quantités considérables d'espace disque supplémentaire sont normalement nécessaires pour le stockage des données.

Installation interactive des composants individuels

Pour installer un ou plusieurs composants individuels sur une installation de Client Automation existante

1. Lancez l'assistant d'installation puis sélectionnez l'option Installer CA ITCM.

   Si une installation existante est détectée, la boîte de dialogue Sélectionner une option d'installation apparaît.

   Sélectionnez l'option Modifier l'installation et suivez les instructions contenues dans l'assistant d'installation.

2. Dans la boîte de dialogue Sélectionner les composants et les fonctionnalités, qui présente toutes les fonctions disponibles, sélectionnez les fonctions à installer.

   Remarque : Les fonctions qui sont déjà installées sont sélectionnées. La désélection d'une fonction existante entraîne sa suppression.

3. Suivez les instructions contenues dans les boîtes de dialogue subséquentes de l'assistant d'installation, puis saisissez les informations nécessaires pour l'installation et la configuration.

Résumé de l'installation

Au cours de l'installation, le programme d'installation collecte des informations sur toutes les opérations effectuées après l'appel du programme de configuration. Un résumé de l'installation fournit une liste des composants que l'utilisateur a sélectionnés pour l'installation. Ce résumé est présenté à l'utilisateur avant le début de l'installation.

Sous Windows, une fois l'installation terminée, le résumé de l'installation est également disponible sous forme de fichier texte appelé DSMSummary.txt. Le fichier texte de résumé de l'installation est enregistré dans le répertoire spécifié par la variable d'environnement %temp%.

Sous Linux et UNIX, le résumé d'installation est conservé dans le fichier journal de l'installation principale, qui est par défaut

/opt/CA/installer/log/ca-dsm.install.log

Retour en arrière de l'installation

Si l'installation d'un des composants appelés par le programme d'installation échoue ou ne peut pas être conclue, un retour en arrière est effectué pour ce package et tous les autres packages qui ont été installés dans le cadre de la session d'installation afin de rétablir un état cohérent du système.

Copie des packages d'installation

Le programme d'installation optimise l'utilisation de l'espace disque en copiant uniquement les packages du support d'installation (DVD) dans le système local ou la bibliothèque de packages logiciels actuellement nécessaires pour la fonction sélectionnée. Considérez les deux cas suivants :

- Si la fonction Déploiement de l'infrastructure a été sélectionnée pour l'installation, les packages d'installation des agents et des serveurs sont copiés du support d'installation dans le système local.
- Si la fonction de gestionnaire Software Delivery est en cours d'installation, tous les packages d'installation, y compris l'explorateur et le gestionnaire DSM, sont copiés dans le dossier AUTOREG de la bibliothèque de packages logiciels.

Dans ces cas, seuls les packages nécessaires à la fonction sélectionnée sont copiés dans le système local et la bibliothèque de packages logiciels. Si toutes les fonctions ont été sélectionnées, l'ensemble des packages sont copiés. Si vous avez uniquement sélectionné la fonction Software Delivery, seuls les packages nécessaires à Software Delivery sont copiés.

Considérations relatives à la norme CCS

Le programme d'installation du gestionnaire DSM choisit automatiquement la variante appropriée de CA Common Services (CCS) : Micro-CCS ou version CCS complète. Si la MDB réside sur Oracle, l'application installe Micro-CCS avec le gestionnaire DSM. La version CCS complète est installée avec une MDB Microsoft SQL Server.

Si vous mettez à niveau le gestionnaire DSM, l'installation du gestionnaire DSM tentera de mettre à niveau la version CCS complète ou Micro-CCS de façon appropriée.

L'option Installer CCS est encore disponible dans le niveau supérieur de l'assistant d'installation de Client Automation. Elle permet d'installer la version CCS complète sur l'ordinateur local. Cette option requiert l'installation de Microsoft SQL Server sur celui-ci, avec une préinstallation de la MDB.

Dans cette version, toutefois, l'option Installer CCS et la MDB a été supprimée du niveau supérieur de l'assistant d'installation de Client Automation.

Installation interactive de CA Client Automation sous Windows

Nous vous recommandons d'exécuter d'abord l'option Vérifier les conditions préalables requises pour vous assurer que les logiciels requis appropriés sont installés avant de commencer l'installation. Consultez les Remarques concernant CCS ici.

Pour installer Client Automation de manière interactive, procédez comme suit :

- Connectez-vous au système en tant qu'administrateur.
- Insérez le DVD d'installation ou exécutez la commande de configuration pour accéder a l'assistant d'installation.
- Suivez les instructions contenues dans l'assistant d'installation, puis saisissez les informations nécessaires pour l'installation et la configuration. L'assistant d'installation propose des explications et des suggestions utiles dans les écrans d'installation.
- La première boîte de dialogue de l'assistant d'installation vous permet de sélectionner la langue utilisée pour l'installation.

L'écran de bienvenue de l'assistant d'installation contient les options suivantes :

Installer Client Automation

Vous permet de choisir les fonctions de produit à installer. Pour cela, vous devez avoir préalablement accepté le contrat de licence.

Installation d'MDB

Vous permet d'installer la base de données de gestion (MDB) sur un hôte dédié, sans aucun des composants de CA Common Services (CCS). Cette MDB sera accessible à distance à tous les composants qui en ont besoin. Cette option d'installation empêche le gestionnaire d'utiliser la fonctionnalité CCS.

Installation d'CCS

Lance une installation interactive de CCS.

Installation de CCS avec la MDB

Démarre l'installation de CCS, ainsi que la base de données de gestion (MDB). Vous devez sélectionner cette option si vous voulez utiliser le gestionnaire DSM avec la fonctionnalité CCS.

Vérifier les conditions préalables

Vérifie l'environnement hôte pour déterminer si l'installation du produit peut être effectuée correctement. L'application vous informera de toutes les conditions externes préalables requises manquantes. Vous devez installer le logiciel requis avant de poursuivre l'installation de Client Automation.

Afficher les documents

Inclut une liste des fichiers de documentation disponibles au format PDF que vous pouvez consulter avec la version gratuite d'Acrobat Reader.

Nous contacter

Inclut l'adresse postale, les adresses Web et électroniques de CA Technologies, y compris les numéros de téléphone et de fax de la société.

Installation interactive sous Linux et UNIX

Pour installer CA Client Automation sous Linux ou UNIX de manière interactive, procédez comme suit :

1. Connectez-vous à l'ordinateur Linux ou UNIX en tant qu'utilisateur root.
2. Insérez le DVD d'installation, puis passez à la racine du DVD et exécutez le script suivant :
   ```
   # sh ./setup.sh
   ```
   L'assistant d'installation est lancé. Assurez-vous de disposer des détails des répertoires dans lesquels vous souhaitez installer les composants.
3. Suivez les instructions contenues dans l'assistant d'installation, puis saisissez les informations nécessaires pour l'installation et la configuration.

La première boîte de dialogue vous permet de sélectionner la langue utilisée pendant l'installation.

La boîte de dialogue de bienvenue suivante offre les options suivantes :

Installation de DSM

Vous permet de choisir les fonctions de produit à installer. Pour cela, vous devez avoir préalablement accepté le contrat de licence.

Afficher les documents

Inclut une liste des fichiers de documentation disponibles au format PDF que vous pouvez consulter avec la version gratuite d'Acrobat Reader.

Nous contacter

Inclut l'adresse postale, les adresses Web et électroniques de CA Technologies, y compris les numéros de téléphone et de fax de la société.

Lorsque vous sélectionnez l'option Installer DSM, l'assistant d'installation vous renvoie d'abord à la boîte de dialogue du contrat de licence de l'utilisateur final (EULA). Après avoir accepté le contrat de licence, vous pouvez sélectionner n'importe quelle combinaison des fonctionnalités suivantes à installer :

- Asset Management
- Remote Control
- Software Delivery

Vous pouvez installer une ou toutes les fonctionnalités et fonctions, même si vous n'avez pas encore acheté de licence pour le produit et exécuter la fonctionnalité pour une période d'essai.

La boîte de dialogue suivante de l'assistant d'installation vous demande de choisir la méthode d'installation.

Remarque : Par défaut, l'assistant d'installation sous Linux ou UNIX est une interface utilisateur graphique (IUG) Java. S'il n'est pas possible d'afficher une interface utilisateur graphique, par exemple, lorsque vous effectuez l'installation à partir d'une console basée sur des caractères, l'assistant d'installation propose une interface utilisateur (basée sur des caractères) de type VT100.

Installation de Client Automation à l'aide de la ligne de commande dans Windows

Les sections suivantes contiennent des informations sur les outils, les packages d'installation et les options d'installation pouvant être utilisés pour effectuer et contrôler l'installation de Client Automation sous Windows via la ligne de commande.

Packages d'installation pour Windows

Le produit CA Client Automation est structuré dans un ensemble de packages MSI pour garantir une distribution et une installation optimales sur le réseau, et réduire le trafic réseau pour le déploiement de l'agent.

L'installation principale contient toutes les boîtes de dialogue du programme d'installation, rassemble les informations nécessaires pour appeler les autres packages en mode silencieux, et gère le retour en arrière si nécessaire. Tous les autres packages installent les fichiers et les ressources nécessaires pour le composant spécifique.

Les produits d'autres fabricants, conditions préalables requises internes pour les composants DSM, sont automatiquement installés à partir de packages MSI distincts.

Les packages d'installation MSI sont enregistrés dans le support d'installation à l'emplacement suivant (*composant* représentant un gestionnaire, l'explorateur, etc.) :

`...\WindowsProductFiles_x86\`*`composant`*

Packages d'installation pour Windows

Le tableau ci-dessous offre un aperçu des packages d'installation disponibles pour CA Client Automation, leurs noms de fichiers et leurs noms affichés dans l'applet Ajout/suppression de programmes du Panneau de configuration Windows.

Les packages d'installation se trouvent dans le dossier WindowsProductFiles_x86 du DVD d'installation CA Client Automation.

Package	Nom du fichier	Nom dans la liste Ajout/suppression de programmes Windows
Configuration principale	setup.exe	CA Client Automation
Explorateur	Explorer.msi	Explorateur DSM CA
Gestionnaire	Manager.msi	Gestionnaire DSM CA
Serveur	Server.msi	Serveur de modularité CA DSM
Agent de base	AgtBHW.msi	Agent DSM CA + module d'extension d'inventaire de base
Agent AM	AgtAM.msi	Agent DSM CA + module d'extension Asset Management
Agent DTS	AgtDTS.msi	Agent DSM CA + module d'extension du service de transport de données
Agent RC	AgtRC.msi	Agent DSM CA + module d'extension Remote Control
Agent SD	AgtRC.msi	Agent DSM CA + module d'extension Software Delivery

Package	Nom du fichier	Nom dans la liste Ajout/suppression de programmes Windows
Documentation	Documentation.msi	Documentation CA DSM
DMPrimer	dmsetup.exe	DMPrimer DSM CA
Serveur ENC :	ServerENC.msi	Serveur ENC CA
RVI	RVI.msi	Inventaire distant de virtualisation CA DSM

Packages d'installation d'autres fabricants

Le tableau ci-dessous offre un aperçu des packages d'installation tiers requis par les composants DSM individuels, leurs noms de fichiers et une description de leur utilité. Pour plus d'informations sur les versions de produit tiers, consultez les avis relatifs aux tiers et contrats de licence disponibles dans la bibliothèque Client Automation.

Package	Nom du fichier	Description
AMS 12.8	setupwin32.exe	Composant CA Technologies pour le système de maintenance des actifs. Requis pour les services Web.
CCS r11.2	setup.exe	Composant CA Technologies pour CA Common Services. Requis pour les installations du gestionnaire.
MDAC	mdac_typ.exe	Package Microsoft Data Access. Requis pour l'accès à la base de données du gestionnaire.
Apache Tomcat 7.0.40		Installation d'Apache Tomcat. Requis pour la console Web.
CA SSA 3.2.0	CA Secure Socket Adapter_NoEtpki.msi	Adaptateur de socket sécurisé CA.
CAPKI 4.3.0	Setup.exe	Les bibliothèques CA PKI

Installation de CA Client Automation à l'aide de setup.exe

Pour installer ou configurer CA Client Automation à partir de la ligne de commande, vous devez démarrer l'installation en exécutant setup.exe à partir du répertoire WindowsProductFiles_x86 du support d'installation (DVD).

Vous pouvez définir les options suivantes lors de l'exécution du programme setup.exe :

/a

Démarre une installation administrative qui décompresse tous les composants et les fichiers DSM dans un partage réseau.

Remarque : Ce paramètre fonctionne uniquement si l'installation est effectuée dans le répertoire de fichiers de produit, et non dans le répertoire racine du support d'installation.

/V"/l*v x:\DSMSetupxxx.log"

Indique le chemin d'accès au fichier journal. Les noms des fichiers journaux sont statiques et ne peuvent donc pas être modifiés.

Outil d'installation msiexec

Les packages d'installation MSI prennent en charge une interface de ligne de commande. Vous pouvez utiliser cette dernière lors du déploiement des fonctions DSM vers des systèmes à distance par d'autres moyens, tels qu'un DVD ou CD personnalisé, ou lors de la conversion de fonctions Client Automation en images de déploiement hôte.

Microsoft Windows Installer (MSI) installe le logiciel à partir de fichiers logiciels dotés de l'extension .msi.

Msiexec.exe est la commande exécutable servant à installer les packages MSI à partir de la ligne de commande. Msiexec est un outil extrêmement flexible offrant de nombreuses options de ligne de commande. Pour une description détaillée des options et paramètres msiexec, consultez l'aide en ligne de Microsoft.

Tous les packages MSI incluent des options générales. Certains packages MSI offrent également des options spécifiques aux packages. Vous pouvez associer ces deux ensembles d'options pour déterminer la manière exacte dont une application particulière doit être installée.

Voici un exemple de commande msiexec utilisant des options générales (/i, -l*v, /qn) et l'option d'installation spécifique au package du gestionnaire ADDLOCAL :

```
msiexec /i "x:\WindowsProductFiles_x86\Manager\Manager.msi" -l*v
"c:\DSMSetupMgr.log" ADDLOCAL=Manager,MgrDC,MgrAM ALLUSERS=1 /qn
```

Les options générales et spécifiques aux packages sont décrites dans les sections Options générales pour msiexec (page 182) etPropriétés MSI spécifique au package (page 184).

Remarque : Les options propres au package de l'agent sont les paramètres d'installation utilisés durant le déploiement interactif pour indiquer les "options d'installation supplémentaires de Windows" sur la page Configuration de l'agent de l'assistant de déploiement. Sur cette page, vous pouvez entrer plusieurs options d'installation séparées par des espaces, afin de remplacer les options existantes.

Important : Si vous installez des composants DSM directement à l'aide de la ligne de commande MSI msiexec, vous devez toujours définir la propriété d'installation MSI ALLUSERS sur la valeur 1 (signifiant "Installe pour tous les utilisateurs mais l'utilisateur requiert des privilèges d'accès administratif sur l'ordinateur") afin de permettre les mises à niveau, désinstallation ou réinstallation ultérieures via la fonction Software Delivery ou Déploiement sur un gestionnaire DSM. Si vous ne définissez pas ce paramètre comme tel ou que vous le conservez vide, le composant est enregistré pour l'utilisateur en question qui l'installe pour la première fois, mais il ne peut être géré à l'aide de fonctions de gestionnaire.

Remarque concernant l'indication de noms de systèmes :

Chaque fois que le programme d'installation Client Automation requiert la saisie d'un nom de système, nous vous recommandons vivement de saisir un nom de domaine complet (FQDN) incluant un suffixe afin de pouvoir atteindre les systèmes informatiques d'autres domaines de réseau, même si la transmission de la requête n'est pas configurée pour tous les DNS impliqués.

Options générales pour msiexec

Tous les packages MSI prennent en charge les options générales suivantes :

/i package d'installation msi

Installe ou configure Client Automation.

/q n|b|r|f|+|–

Définit le niveau de l'interface utilisateur.

Option (combinaison)	Niveau de l'interface utilisateur
q	Aucune interface utilisateur

Option (combinaison)	Niveau de l'interface utilisateur
qn	Aucune interface utilisateur
qb	Interface utilisateur standard. Utilisez qb! pour masquer le bouton Annuler.
qr	Interface utilisateur réduite, sans boîte de dialogue modale affichée à la fin de l'installation.
qf	Interface utilisateur complète, avec boîtes de dialogue modales Erreur irrécupérable, Quitter utilisateur ou Quitter créées à la fin.
qn+	Aucune interface utilisateur, à l'exception d'une boîte de dialogue modale affichée à la fin.
qb+	Interface utilisateur standard, avec boîte de dialogue modale affichée à la fin. La boîte de dialogue modale n'apparaît pas si l'utilisateur annule l'installation. Utilisez qb+! ou qb!+ pour masquer le bouton Annuler.
qb–	Interface utilisateur standard, sans boîte de dialogue de fin modale. Le niveau d'interface utilisateur /qb+- n'est pas pris en charge. Utilisez qb–! ou qb!- pour masquer le bouton Annuler.

Remarque : Le point d'exclamation (!) est disponible avec Microsoft Windows Installer 2.0 et fonctionne uniquement avec l'interface utilisateur standard. Elle n'est pas valide avec l'interface utilisateur complète.

/l [i|w|e|a|r|u|c|m|o|p|v|x|+|!|*] ***fichierjournal***

Ecrit des informations de connexion dans un fichier journal au chemin spécifié. Des indicateurs décrivent les informations à consigner dans le journal. Si aucun indicateur n'est spécifié, la valeur par défaut est iwearmo.

Indicateur	Informations à consigner dans le journal
i	Messages d'état
w	Avertissements non irrécupérables
E	Tous les messages d'erreur
a	Démarrage des actions
P	Enregistrements propres à une action
u	Requêtes de l'utilisateur
c	Paramètres initiaux de l'interface utilisateur
m	Informations liées à une quantité de mémoire insuffisante ou à une fermeture irrécupérable
o	Messages liés à un espace disque insuffisant
p	Propriétés du terminal

Indicateur	Informations à consigner dans le journal
t	Sortie en mode prolixe
x	Informations de débogage supplémentaires. Disponible uniquement sur Windows Server 2003
+	Ajout au fichier existant
!	Vidage de chaque ligne dans le fichier journal
*	Caractère générique. Consignation de toutes les informations, à l'exception des options v et x. Pour inclure les options v et x, spécifiez /l*vx

Propriétés MSI propres aux packages

Les packages d'installation MSI des composants DSM et des modules d'extension suivants prennent en charge les propriétés d'installation propres aux packages :

- explorateur DSM
- Agent d'inventaire de base
- Agent de gestion d'actifs
- Agent de service de transport de données
- Agent Remote Control
- Agent Software Delivery
- Serveur de modularité
- Gestionnaire
- Serveur de passerelle ENC

Remarque : Vous devez transférer les propriétés MSI spécifiques des packages en tant que paramètres d'utilisateur dans votre job logiciel. Pour plus d'informations sur les paramètres d'utilisateur, consultez la rubrique Onglet Jobs dans la section Software Delivery de l'*Aide de l'explorateur DSM*.

Conditions d'installation requises pour les packages MSI

Avant d'installer l'un des packages MSI, il est nécessaire d'installer les bibliothèques ETPKI et l'adaptateur de socket sécurisé CA. Pour connaître les versions requises de ces conditions préalables, consultez la section Packages d'installation d'autres fabricants. (page 180)

- **Installation des bibliothèques CAPKI :**

  L'installation de CAPKI se trouve sur le support d'installation de Client Automation (CD/DVD) dans le répertoire WindowsProductFiles_x86\CAPKI.

  Pour installer les bibliothèques CAPKI, utilisez la ligne de commande suivante :

  ```
  setup install caller=CADSMCAPKI
  ```

- **Installation de l'adaptateur de socket sécurisé CA :**

  L'adaptateur de socket sécurisé CA peut être installé à l'aide de son programme d'installation, situé dans le répertoire WindowsProductFiles_x86\SSA sur le support d'installation de CA Client Automation (CD/DVD).

  Pour installer l'adaptateur de socket sécurisé CA, utilisez la ligne de commande suivante :

  ```
  msiexec.exe
  /i"D:\WindowsProductFiles_x86\SSA\CASockAdapterSetupWin32NoEtpki.msi" /l*v
  "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DSMSetupSSA.log" /qb-!
  ```

Propriétés MSI propres au package Explorateur

Le package d'installation MSI de l'explorateur DSM (Explorer.msi) prend en charge les propriétés propres aux packages suivantes :

ADDLOCAL

Fonctions spécifiques pouvant être sélectionnées pour l'installation.

Valeur	Description
Explorateur	Composants communs de l'explorateur (obligatoires pour l'installation de l'explorateur)
ExpAM	Module d'extension Asset Management
ExpRC	Module d'extension commun Remote Control
ExpSD	Module d'extension commun Software Delivery
ExpSDB	Module d'extension Boot Manager
ExpSDM	API client du gestionnaire Software Delivery
ExpRP	Module d'extension Reporter

Valeur	Description
TOUT	Sélectionne toutes les fonctions mentionnées plus haut.

ADMINCONSOLE_MANAGER

Système de gestion auquel l'explorateur DSM doit se connecter.

Valeur : Nom ou adresse IP du système

Propriétés MSI pour le package de l'agent d'inventaire de base

Le package d'installation MSI du module d'extension de l'agent de l'inventaire de base (AgtBHW.msi) et le client ENC prennent en charge les propriétés propres aux packages suivantes :

AGENT_SERVER

Serveur de modularité auquel l'agent doit se connecter.

Valeur : Nom ou adresse IP du système

AGENT_DEFAULTGROUPS

Groupe ou liste de groupes de gestion créés au niveau du gestionnaire auprès duquel l'agent s'enregistre automatiquement.

Valeur : Liste séparée par des virgules de noms de groupe

Exemple : Grp1/subgroup1,Group2,...

ENC_CLIENT_ENABLED

Indique si le client ENC doit être activé lors de l'installation de l'inventaire matériel de base. Par défaut, les fichiers du client sont copiés sur l'ordinateur mais ne sont pas exécutés. Cela simplifie le programme d'installation et permet un job de configuration simple pour activer le client ultérieurement, le cas échéant.

Valeur : 0 (laisser inactif), 1 (rendre actif)

Remarque : Les paramètres suivants *n'ont pas besoin* d'être précisés si le client ENC n'est pas activé.

ENC_SVR_ADDR

Le serveur de passerelle ENC auquel ce client doit se connecter.

Valeur : FQN du serveur

ENC_SVR_TCP_PORT

Port TCP du serveur de passerelle ENC auquel se connecter.

Valeur par défaut : 443

ENC_SVR_HTTP_PORT

Port HTTP du serveur de passerelle ENC auquel se connecter.

Valeur par défaut : 80

ENC_HTTP_PROXY_ADDR

Adresse d'un proxy Internet HTTP auquel le client ENC doit se connecter afin de se connecter en-dehors du réseau local.

ENC_HTTP_PROXY_PORT

Numéro du port sur le proxy auquel se connecter.

Valeur par défaut : 8080

ENC_PROXY_ORDER

Ensemble de types de connexions tentées par le client ENC. Si ce paramètre est omis, un ordre par défaut est utilisé.

Valeur : Cette liste séparée par des espaces est composée d'aucun ou de plusieurs mots-clés suivants : socket, socks4Anon, socks5Auth, socks5Anon, httpConnect, http et httpProxy

ENC_SOCKS_ADDR

Adresse d'un proxy Internet SOCKS auquel le client ENC doit se connecter afin de se connecter en-dehors du réseau local.

Valeur : Adresse FQN ou IP du serveur

ENC_SOCKS_PORT

Numéro du port sur le proxy auquel se connecter.

Valeur par défaut : 1080

ENC_SOCKS_USER

Nom de l'utilisateur à authentifier lors de la connexion au serveur SOCKS.

Exemple : utilisateursocks

ENC_SOCKS_PW

Mot de passe en texte brut de l'utilisateur indiqué par ENC_SOCKS_USER.

ENC_HTTP_PROXY_USER

Nom de l'utilisateur à authentifier lors de la connexion au serveur HTTP.

Exemple : utilisateurhttp

ENC_HTTP_PROXY_PW

Mot de passe en texte brut de l'utilisateur indiqué par ENC_HTTP_PROXY_USER.

Remarque : Pour plus d'informations sur les propriétés ENC, consultez le document *Référence de la commande encUtilCmd.* Consultez également la rubrique Groupe de stratégies de la passerelle ENC dans la section Stratégie de configuration de *l'aide de l'explorateur DSM.*

Propriétés MSI pour le package de l'agent Asset Management

Le package d'installation MSI du module d'extension de l'agent Asset Management (AgtAM.msi) prend en charge les propriétés propres aux packages suivantes :

AGENT_SERVER

Serveur de modularité auquel l'agent doit se connecter.

Valeur : Nom ou adresse IP du système

AGENT_DEFAULTGROUPS

Groupe ou liste de groupes de gestion créés au niveau du gestionnaire auprès duquel l'agent s'enregistre automatiquement.

Valeur : Liste séparée par des virgules de noms de groupe

Exemple : Grp1/subgroup1,Group2,...

Propriétés MSI pour le package de l'agent de service de transport de données

Le package d'installation MSI du module d'extension de l'agent de service de transport de données (DTS) (AgtDTS.msi) prend en charge les propriétés propres aux packages suivantes :

SC_DSMPROP

Raccourci vers la boîte de dialogue de propriétés de l'agent.

Valeur	Description
1	Un raccouci vers la boîte de dialogue de propriétés de l'agent est introduit dans le menu Démarrer.
0	Aucun raccourci n'est créé.

ADDLOCAL

Fonctions spécifiques pouvant être sélectionnées pour l'installation.

Valeur	Description
Agent	Composants communs de l'agent (obligatoires pour toute installation d'agent)
AgtDTS	Composants communs de l'agent de service de transport de données(obligatoires pour l'installation de l'agent DTS)
ALL	Sélectionne toutes les fonctions mentionnées plus haut.

AGENT_DEFAULTGROUPS

Groupe ou liste de groupes de gestion créés au niveau du gestionnaire auprès duquel l'agent s'enregistre automatiquement.

Valeur : Liste séparée par des virgules de noms de groupe

Exemple : Grp1/subgroup1,Group2,...

Propriétés MSI pour le package de l'agent Remote Control

Le package d'installation MSI du module d'extension de l'agent Remote Control (AgtRC.msi) prend en charge les propriétés propres aux packages suivantes :

SC_DSMPROP

Raccourci vers la boîte de dialogue de propriétés de l'agent.

Valeur	Description
1	Un raccouci vers la boîte de dialogue de propriétés de l'agent est introduit dans le menu Démarrer.
0	Aucun raccourci n'est créé.

ADDLOCAL

Fonctions spécifiques pouvant être sélectionnées pour l'installation.

Valeur	Description
Agent	Composants communs de l'agent (obligatoires pour toute installation d'agent)

Valeur	Description
AgtRC	Composants communs de l'agent de contrôle à distance (obligatoires pour l'installation de l'agent Remote Control)
AgtRCA	Hôte Remote Control
AgtRCV	Visionneuse Remote Control
AgtRCP	Module de relecture Remote Control
TOUT	Sélectionne toutes les fonctions mentionnées plus haut.

AGENT_SERVER

Serveur de modularité auquel l'agent doit se connecter.

Valeur : Nom ou adresse IP du système

RC_AGENT_STANDALONE

Valeur	Description
0	L'agent Remote Control est géré de manière centralisée
1	L'agent Remote Control est autonome

AGENT_DEFAULTGROUPS

Groupe ou liste de groupes de gestion créés au niveau du gestionnaire auprès duquel l'agent s'enregistre automatiquement.

Valeur : Liste séparée par des virgules de noms de groupe

Exemple : Grp1/subgroup1,Group2,...

Propriétés MSI pour le package de l'agent Software Delivery

Le package d'installation MSI du module d'extension de l'agent Software Delivery (AgtSD.msi) prend en charge les propriétés propres aux packages suivantes :

SC_DSMPROP

Raccourci vers la boîte de dialogue de propriétés de l'agent.

Valeur	Description
1	Un raccouci vers la boîte de dialogue de propriétés de l'agent est introduit dans le menu Démarrer.

Valeur	Description
0	Aucun raccourci n'est créé.

ADDLOCAL

Fonctions spécifiques pouvant être sélectionnées pour l'installation.

Valeur	Description
Agent	Composants communs de l'agent (obligatoires pour toute installation d'agent)
AgtSD	Composants communs de l'agent Software Delivery (obligatoires pour l'installation de l'agent Software Delivery)
AgtSDA	Composants Software Delivery (obligatoires pour le catalogue SD)
AgtSDC	Composants du catalogue Software Delivery
TOUT	Sélectionne toutes les fonctions mentionnées plus haut.

AGENT_SERVER

Serveur de modularité auquel l'agent doit se connecter.

Valeur : Nom ou adresse IP du système

AGENT_DEFAULTGROUPS

Groupe ou liste de groupes de gestion créés au niveau du gestionnaire auprès duquel l'agent s'enregistre automatiquement.

Valeur : Liste séparée par des virgules de noms de groupe

Exemple : Grp1/subgroup1,Group2,...

Propriétés MSI pour le package du serveur de modularité

Le package d'installation MSI du serveur de modularité (Server.msi) prend en charge les propriétés propres aux packages suivantes :

FIPS_MODE

Indique le mode FIPS défini par le programme d'installation de Client Automation.

Valeur	Description
1	Préférence FIPS

Valeur	Description
2	FIPS uniquement

ADDLOCAL

Fonctions spécifiques pouvant être sélectionnées pour l'installation.

Valeur	Description
Serveur	Composants communs du serveur de modularité (obligatoires pour toute installation de serveur)
SrvAM	Module d'extension de modularité Asset Management
SrvSD	Module d'extension de serveur de modularité Software Delivery
SrvRC	Module d'extension de serveur de modularité Remote Control
ALL	Sélectionne toutes les fonctions mentionnées plus haut.

SRV_SDBPATH

Chemin du répertoire dans lequel doit être installée la base de données du serveur de modularité.

SERVER_PATH

Chemin du répertoire dans lequel doivent être installées les données propres du serveur de modularité.

SERVER_MANAGER

Système de gestion auquel le serveur de modularité doit se connecter.

Valeur : Nom ou adresse IP du système

SERVER_ENGINE

Système moteur auquel le serveur de modularité doit se connecter. Si ce paramètre n'est pas spécifié, le moteur du système est pris en compte par défaut.

Valeur : nom du moteur

BS_OS_PATH

Chemin du répertoire dans lesquel sont stockées les images du système d'exploitation et d'autres données propres au serveur de démarrage. Le chemin doit se terminer par la chaîne \SDBS\var.

Exemple : f:\Program Files\CA\DSM\Server\SDBS\var

CREATESDMSISHARE

Partage pour l'accès aux packages MSI enregistrés dans le gestionnaire Software Delivery.

Valeur	Description
1	Crée un partage pour l'accès aux packages MSI.
0	Ne crée pas de partage SERVER_ENGINE.

CREATESDLIBSHARE

Partage pour l'accès aux packages enregistrés dans la bibliothèque de packages logiciels.

Valeur	Description
1	Crée un partage pour l'accès aux packages.
0	Ne crée pas de partage.

BOOTSERVER_ENABLED

Détermine l'activation ou non du service Serveur de démarrage.

Valeur	Description
0	N'active pas le service Serveur de démarrage.
1	Active le service Serveur de démarrage.

BOOTSERVER_DISABLESHARES

Partage pour l'accès aux packages enregistrés dans le Boot Server.

Valeur	Description
0	Crée un partage pour l'accès aux packages.
1	Ne crée pas de partage.

Propriétés MSI pour le package Gestionnaire

Le package d'installation MSI du gestionnaire (Manager.msi) prend en charge les propriétés propres aux packages suivantes :

ADDLOCAL

Fonctions spécifiques pouvant être sélectionnées pour l'installation.

Valeur	Description
Gestionnaire	Composants communs du gestionnaire (obligatoires pour toute installation de gestionnaire)
MgrInf	Infrastructure commune du gestionnaire (obligatoires pour toute installation de gestionnaire)
MgrDC	Module d'extension du moteur (obligatoire pour toute installation de gestionnaire)
MgrAM	Module d'extension du gestionnaire Asset Management
MgrRC	Module d'extension du gestionnaire Remote Control
MgrSD	Module d'extension du gestionnaire Software Delivery
MgrDTS	Module d'extension du gestionnaire de service de transport de données (obligatoire pour toute installation du gestionnaire Software Delivery)
MgrDM	Module d'extension du gestionnaire Deployment
MgrIP	Module d'extension du gestionnaire Image Prepare
TOUT	Sélectionne toutes les fonctions mentionnées plus haut.

DMSOFTLIBDIR

Chemin du répertoire dans lequel doivent être installés les packages pour DMDeploy.

DMKEYLOCATION

Chemin du répertoire du fichier clé du gestionnaire de déploiement.

SDLIBRARY

Chemin du répertoire dans lequel doit être installée la bilbiothèque de packages logiciels.

MANAGER_ROLE

Rôle du gestionnaire.

Valeur	Description
0 = Entreprise	Le gestionnaire joue le rôle de gestionnaire d'entreprise.
1 = Membre du domaine	Le gestionnaire joue le rôle de gestionnaire de domaine au sein d'une entreprise.
2 = Gestionnaire autonome	Le gestionnaire joue le rôle de gestionnaire de domaine autonome.

ENTERPRISE_NAME

Système de gestion d'entreprise auquel doit se connecter le gestionnaire de domaines si le rôle Membre du domaine (valeur = 1) a été défini. Sinon, la propriété est vide.

Valeur : Nom ou adresse IP du système

WAC_MANAGER

Système de gestionnaire de console Web pour une installation de console Web autonome.

Valeur : Nom ou adresse IP du système

ENGINE_MANAGER

Système de gestionnaire de moteur pour une installation de moteur autonome.

Valeur : Nom ou adresse IP du système

DSM_TOMCAT_PORT

Port TCP/IP où le gestionnaire écoute les demandes.

Valeur par défaut : 8090

DSM_TOMCAT_SHUT

Port TCP/IP où le gestionnaire écoute les demandes d'arrêt.

Valeur par défaut : 8095

DSM_TOMCAT_AJP

Port sur lequel le travail écoute les demandes Ajp13, afin de les transmettre aux travaux hors processus à l'aide du protocole Ajpv13.

Valeur par défaut : 8020

DB

Type de la base de données utilisée.

Valeur : SQLServer ou Oracle

DBSERVER

Nom du système dans lequel réside la base de données.

Valeur : Nom ou adresse IP du système

DBUSERNAME

Nom d'utilisateur Windows pour l'accès à la base de données.

DBPASSWORD

Mot de passe pour DBUSERNAME.

DBVUSER

Vnode sur le système de base de données si la base de données est Ingres et si un système de base de données distant est utilisé.

DBVPWD

Mot de passe pour DBVUSER.

DBSW

Indicateurs si des signatures logicielles pour la détection logicielle doivent être insérées (incluses) ou non (exclues) dans la base de données de gestion.

Valeur	Description
excl_sw	Ne pas insérer de signatures logicielles.
incl_sw	Insérer des signatures logicielles.

FAILOVER_ENABLED

Attribuer un indicateur si la prise en charge de la récupération est activée ou désactivée.

Valeur	Description
0	La prise en charge de la récupération est désactivée.
1	La prise en charge de la récupération est activée.

FAILOVER_STATUS

Attribuer un indicateur si ce gestionnaire constitue le noeud actif ou passif dans un environnement en cluster.

Valeur	Description
0	Ce gestionnaire est un gestionnaire passif.
1	Ce gestionnaire constitue le gestionnaire actif.

FAILOVER_CLUSTER_NAME

Nom de cluster du gestionnaire.

Propriétés MSI pour le package Serveur de passerelle ENC

Le package d'installation MSI du serveur de passerelle ENC prend en charge les propriétés propres aux packages suivantes :

AGENT_SERVER

Serveur de modularité auquel l'agent doit se connecter.

Valeur : Nom ou adresse IP du système

ENC_CLIENT_ENABLED

Indique si le client ENC doit être activé lors de l'installation du serveur de passerelle ENC.

Valeur : 0 (laisser inactif), 1 (rendre actif)

ENC_SERVER_TYPE

Indique les rôles du serveur de passerelle ENC. Cela inclut une ou plusieurs des valeurs répertoriées dans le tableau ci-dessous, séparées par des espaces. Un serveur de passerelle ENC peut fonctionner dans un ou plusieurs rôles. Si un gestionnaire est indiqué, un serveur est automatiquement configuré. Le client ENC est également automatiquement configuré pour s'enregistrer auprès de ce serveur.

Si un seul Serveur de passerelle ENC est configuré, le client s'enregistre également auprès de celui-ci.

Dans les deux cas ci-dessus, les paramètres de configuration pour le client ne sont pas requis, à l'exception de ENC_CLIENT_ENABLED.

Si un seul routeur est configuré, le client et le routeur doivent tous deux s'enregistrer auprès d'un autre serveur de passerelle ENC. Pour cela, utilisez le paramètre ENC_SVR_ADDR.

Valeur	Description
ENC_SRS	Configurez-le pour fonctionner comme serveur d'enregistrement de passerelle ENC.
ENC_ROUTER	Configurez-le pour fonctionner comme routeur de passerelle ENC.
ENC_MRS	Configurez-le pour fonctionner comme gestionnaire d'enregistrement de passerelle ENC.

ENC_SVR_ADDR

Si vous installez un routeur de passerelle ENC, celui-ci doit être le serveur de passerelle ENC auprès duquel il s'enregistrera.

Si vous installez un serveur d'enregistrement de passerelle ENC, celui-ci doit être le gestionnaire d'enregistrement de passerelle ENC auprès duquel il s'enregistrera.

Valeur : FQN du serveur ou gestionnaire de passerelle ENC auprès duquel s'enregistrer.

Remarque : Si vous installez un gestionnaire de passerelle ENC, la configuration est automatique.

ENC_SVR_TCP_PORT

Port TCP du gestionnaire de passerelle ENC auquel se connecter.

Valeur par défaut : 443

Remarque : Si vous installez un gestionnaire de passerelle ENC, la configuration est automatique.

ENC_SVR_HTTP_PORT

Port HTTP du gestionnaire de passerelle ENC auquel le serveur ou le routeur d'enregistrement de passerelle ENC se connectera.

Valeur par défaut : 80

Remarque : Si vous installez un gestionnaire d'enregistrement de passerelle ENC, la configuration est automatique. Ce paramètre doit uniquement être configuré pour les serveurs ou routeurs de passerelle.

Remarque : Pour plus d'informations sur les propriétés ENC, consultez le document *Référence de la commande encUtilCmd.* Consultez également la rubrique Groupe de stratégies de la passerelle ENC dans la section Stratégie de configuration de *l'aide de l'explorateur DSM.*

Propriétés complémentaires pour msiexec

Les propriétés suivantes sont communes à tous les packages d'installation MSI fournis par CA Technologies :

CA

Répertoire d'installation sur le système cible.

Exemple : C:\Program Files\CA

CONFIGDATA_LOCATION

Répertoire d'installation pour les données de configuration du package, y compris le magasin de configuration (comstore).

Par défaut : Répertoire d'installation du produit.

Exemple : C:\Program Files\CA\DSM

SHAREDCOMPONENTS

Répertoire d'installation pour les composants partagés du package.

Exemple : C:\Program Files\CA\SC

Remarque : **Une fois un package installé, les valeurs de ces propriétés communes sont fixes pour tous les autres packages installés ultérieurement.**

Pour chaque package d'installation MSI, vous pouvez en plus utiliser les propriétés suivantes :

DSM_LANGUAGE

Indique la langue de l'installation de CA Client Automation. Les valeurs possibles sont : enu (anglais), deu (allemand), fra (français) et jpn (japonais).

Les fichiers de toutes les versions linguistiques prises en charges de CA Client Automation sont installés, mais la langue indiquée par DSM_LANGUAGE est utilisée en tant que langue pour l'installation en cours.

Par défaut : Vide (NULL) Cela force le programme d'installation à utiliser l'environnement linguistique par défaut. Si l'environnement linguistique par défaut du système ne figure pas parmi les environnements pris en charge, enu (anglais) est utilisé.

Remarque : DSM_LANGUAGE n'indique par la langue des boîtes de dialogue de l'assistant d'installation.

REBOOT

Valeur	Description
REALLYSUPPRESS	Si un redémarrage est nécessaire, il le supprimera dans tous les cas et nécessitera une exécution manuelle.

ALLUSERS

Valeur	Description
0	Réalise l'installation pour un utilisateur particulier.
1	Permet d'effectuer l'installation pour tous les utilisateurs, mais ils doivent avoir les privilèges d'accès administratifs sur l'ordinateur.
2	Réalise l'installation pour tous les utilisateurs si l'utilisateur a un accès administratif, sinon, cette valeur réalise l'installation pour un utilisateur particulier

Remarque : Si vous installez des composants DSM directement à l'aide de la ligne de commande MSI, vous devez toujours définir le paramètre ALLUSERS=1 afin d'autoriser toute mise à niveau, désinstallation ou réinstallation ultérieure via Software Delivery ou la fonctionnalité Déploiement en-dehors d'un gestionnaire. Si vous ne définissez pas ce paramètre comme tel ou que vous le conservez vide, le composant est enregistré pour l'utilisateur en question qui l'installe pour la première fois, mais il ne peut être géré à l'aide des fonctions du gestionnaire.

ARPSYSTEMCOMPONENT

La définition de cette propriété empêche l'affichage de l'application dans la liste Ajout/Suppression de programmes du Panneau de configuration Windows. Cette propriété n'a aucun effet sur l'environnement d'exécution antérieur à Windows 2000 et Windows XP.

CAF_INSTALL_SERVICE

Valeur	Description
0 | 1	Doit être 1 pour le premier package MSI que vous installez sur le système. Pour tous les autres, la valeur peut être 0.

CAF_START_SERVICE

Valeur	Description
0 | 1	Doit être 1 pour le dernier package MSI que vous installez sur le système. Pour tous les autres, la valeur doit être 0.

FIPS_MODE

Valeur	Description
1	Installation de Client Automation dans le mode -Préférence FIPS (mode par défaut)
2	Installation de Client Automation dans le mode -FIPS uniquement

Options de msiexec pour la désinstallation, la réparation et l'installation administrative

Vous pouvez également utiliser l'interface de ligne de commande MSI pour lancer des tâches de désinstallation, de réparation ou d'installation administrative :

/x msi_install_package | code produit

Désinstalle un produit.

/f [p|o|e|d|c|a|u|m|s|v] msi_install_package | code produit

Répare un produit. Cette option ignore les valeurs de propriété entrées sur la ligne de commande. La liste des arguments par défaut pour cette option est « omus ». Cette option partage la même liste d'arguments que la propriété REINSTALLMODE.

Option	Description
p	Réinstalle uniquement si un fichier est manquant.
o	Réinstalle si un fichier est manquant ou si une version antérieure est installée.
E	Réinstalle si un fichier est manquant ou si une version identique ou antérieure est installée.
j	Réinstalle si un fichier est manquant ou si une version différente est installée.
c	Reinstalle si un fichier est manquant ou si la somme de contrôle stockée ne correspond pas à la valeur calculée. Répare uniquement les fichiers qui ont msidbFileAttributesChecksum dans la colonne Attributs de la table Fichier.
a	Force la réinstallation de tous les fichiers.
u	Réécrit toutes les entrées de registre propres à l'utilisateur requises.
m	Réécrit toutes les entrées de registre propres à l'ordinateur requises.
s	Ecrase tous les raccourcis existants.
t	Exécute à partir de la source et remet le package local en mémoire cache. N'utilisez pas l'option de réinstallation v pour la première installation d'une application ou fonction.

/a msi_install_package

Option d'installation administrative. Installe un produit sur un partage réseau, à partir de l'emplacement auquel il peut être installé sur le réseau.

Exemple de combinaison des options et propriétés msiexec

L'exemple suivant vous montre comment vous pouvez combiner des options et des propriétés msiexec.

```
msiexec.exe
/i"N:\DSM_11_2_9999_0_DVD\WindowsProductFiles_x86\Manager\Manager.msi"
/l*v "G:\DOCUME~1\KSYST0~1,TAN\LOCALS~1\Temp\DSMSetupManager.log"
ADDLOCAL=Manager,MgrAM,MgrRC,MgrSD,MgrDC,MgrDTS,MgrDM,MgrIP
REBOOT=REALLYSUPPRESS ALLUSERS=1
CA="G:\Program Files\CA\DSM\"
CAF_INSTALL_SERVICE="1" CAF_START_SERVICE="0"
/qb-! DMSOFTLIBDIR="G:\Program Files\CA\DSM"
SDLIBRARY="G:\Program Files\CA\DSM\SD\ASM\LIBRARY"
ENTERPRISE_NAME="KSYST01U"
MANAGER_ROLE="2" DB="SQLServer"
DBSERVER="KSYST01U" DBUSERNAME="ca_itrm" DBPASSWORD=XXX DBSW="excl_sw"
```

Installation de Client Automation à l'aide de la ligne de commande dans Linux ou UNIX

Vous installez Client Automation sur Linux ou UNIX à l'aide du script installdsm, qui est situé dans le répertoire de distribution sous LinuxProductFiles_x86/component.

Remarque : CADSMCMD est fourni uniquement pour Linux, et non pour d'autres systèmes dérivés d'UNIX. Pour plus d'informations, reportez-vous au *Manuel de référence des composants CLI*.

Pour des raisons pratiques et de cohérence avec l'installation Windows, il existe un fichier script appelé setup.sh dans le répertoire racine du DVD d'installation. Ce script appelle /LinuxProductFiles_x86/manager/installdsm.

Par défaut, le programme d'installation pour Linux et UNIX s'exécute en mode interactif. Si Client Automation est déjà installé sur le système, le programme d'installation vous permet de choisir des options de mise à niveau, de réparation, de modification ou de désinstallation.

Le média d'installation contient également un fichier de réponse modèle (install.rsp). Ce fichier peut être utilisé pour créer des installations non gérées.

Installation du script Installer Client Automation sur Linux ou UNIX

Le script installdsm a le format suivant :

```
installdsm [-f | -r responsefile [/Rname=value…] | -g responsefile ]
```

-f

Force l'installation sans sauvegarde d'une version du produit antérieure éventuelle.

-r *fichierréponse* [/R*name*=*valeur* ...]

Exécute une installation autonome à l'aide des valeurs spécifiées dans le fichier de réponse. L'option -r option permet à installdsm de vérifier que le fichier de réponse n'est pas vide et qu'il contient un ensemble valide de paires étiquette-valeur. La spécification /R écrase tous les paramètres spécifiés dans le fichier de réponse. Indiquez une spécification /R distincte pour chaque paramètre que vous souhaitez écraser, par exemple :

```
installdsm -r rsp.txt \
/RITRM_AUTOSTART_INSTALL=1 \
/RITRM_AUTOSTART_REBOOT=1
```

Aucune vérification n'est effectuée sur la validité des noms ou des valeurs de paramètres ou si les paramètres indiqués se trouvent dans le fichier de réponse.

La liste par défaut des paramètres est fournie en tant que fichier de réponse échantillon install.rsp dans chacun des packages Linux et UNIX.

Chaque fois que vous utilisez le programme d'installation pour une installation interactive ou pour générer un fichier de réponse pour une installation autonome, vous pouvez éditer les valeurs des paramètres. Après l'installation, le script vous invite à entrer les options, le programme copie les fichiers à l'emplacement et exécute les actions de configuration.

-g *fichierréponse*

Génère un fichier de réponse. Le script affiche les boîtes de dialogue pour une installation interactive, mais écrit, à la fin de la séquence des boîtes de dialogue, tous les valeurs de propriété que vous spécifiez dans le fichier de réponse indiqué.

Paramètre du fichier de réponse dans Linux et UNIX

Une installation autonome de Client Automation est gérée par un fichier de réponse. Le fichier de réponse est un fichier texte qui contient des valeurs de paramètre contrôlant l'installation et la configuration. Le fichier de réponse est généré avant l'installation, soit manuellement, soit à l'aide du script installdsm avec l'option -g. Pendant l'installation, le fichier de réponse est en lecture seule.

L'installation Client Automation comprend des fichiers de réponse standard que vous pouvez utiliser pour exécuter une installation autonome. Le dossier de chaque composant contient un fichier install.rsp. Le fichier de réponse échantillon permet une installation complète du composant.

Modification des valeurs de propriété de l'installation

Le fichier de réponse contient des valeurs de paramètre (propriétés) contrôlant l'installation et la configuration initiale.

La plupart des paramètres Client Automation possèdent le préfixe CA_ITRM, CA_DSM, ITRM_ ou DSM_ ou bien un préfixe indiquant le composant. D'autres paramètres peuvent être utilisés par d'autres produits CA.

Vous pouvez remplacer les valeurs de paramètre dans le fichier de réponse en utilisant installdsm avec la spécification /R. Cela vous permet de modifier le comportement de l'installation par défaut lors d'installations distantes exécutées à l'aide de l'assistant Déploiement de l'infrastructure ou des packages Software Delivery.

Si vous modifiez manuellement un fichier de réponse, soyez attentifs aux valeurs de propriétés généralement dérivées d'autres valeurs de propriétés (principalement des emplacements de répertoires et sous-répertoires). Ne pré-programmez pas une valeur de propriété précédemment dérivée d'une autre afin de ne pas séparer une liaison de dérivation.

Exemple

SDLIBRARY (emplacement de la bibliothèque Software Delivery) dérive par défaut de CA_DSM_CONFIGDATA (emplacement des données de configuration de Client Automation), qui dérive lui-même de CA_ITRM_BASEDIR (emplacement principal de Client Automation). Ces relations sont gérées dans le fichier de réponse install.rsp fourni. Dans un fichier de réponse, si CA_DSM_CONFIGDATA est préprogrammé comme suit : CA_DSM_CONFIGDATA=/data/CA/ConfigDataLocation et que SDLIBRARY est préprogrammé ainsi SDLIBRARY=/data/CA/SDLibrary, les liaisons de dérivation entre CA_ITRM_BASEDIR, CA_DSM_CONFIGDATA et SDLIBRARY sont rompues.

Remarque : Les options propres au package de l'agent sont les paramètres d'installation utilisés durant le déploiement interactif pour indiquer les "options d'installation supplémentaires de UNIX" sur la page Configuration de l'agent de l'assistant de déploiement. Sur cette page, vous pouvez entrer plusieurs options d'installation séparées par des espaces, afin de remplacer les options existantes.

Propriétés d'installation de base

CA_ITRM_BASEDIR

Spécifie le répertoire d'installation du produit. Seuls les composants DSM sont stockés dans ce répertoire. Les composants partagés avec d'autres produits CA Technologies sont stockés dans un répertoire sur lequel pointe la variable d'environnement $CASHCOMP. Tous les composants DSM doivent utiliser la même valeur pour $CA_ITRM_BASEDIR. Par conséquent, si vous déployez des agents DSM à l'aide de l'assistant Déploiement de l'infrastructure ou de la ligne de commande à partir d'un gestionnaire de domaine, vous devez spécifier la valeur requise pour CA_ITRM_BASEDIR dans les arguments pour le composant DMPrimer, qui correspond généralement au premier composant DSM à être installé sur un ordinateur. Pour plus d'informations, reportez-vous à la section Envoi d'options vers l'installation DMPrimer (page 255).

Valeur par défaut : /opt/CA/DSM

CA_DSM_CONFIGDATA

Indique le répertoire d'installation des données de configuration.

Par défaut : $CA_ITRM_BASEDIR

CASHCOMP

Spécifie le répertoire parent pour les composants communs et répertoires de liaison. Si cette variable a été définie par d'autres composants actuellement installés, elle reste inchangée. Les variables d'environnement $CALIB et $CABIN sont dérivées de CASHCOMP. Tous les composants logiciels CA Technologies doivent utiliser la même valeur pour $CASHCOMP sur un ordinateur spécifique. Par conséquent, si vous déployez des agents DSM à l'aide de l'assistant Déploiement de l'infrastructure ou de la ligne de commande à partir d'un gestionnaire de domaine, vous devez spécifier la valeur requise pour CASHCOMP dans les arguments relatifs à l'installation DMPrimer, qui est généralement le premier composant DSM installé sur un ordinateur. Pour plus d'informations, reportez-vous à la section Envoi d'options vers l'installation DMPrimer (page 255).

Valeur par défaut : /opt/CA/SharedComponents

DSM_ALLOW_SOFT_PREREQS

Spécifie si l'installation doit se poursuivre même si la vérification des logiciels requis échoue. Indiquez 1 pour forcer l'installation même s'il manque des logiciels requis.

Important : La désactivation de la vérification des logiciels requis peut entraîner une installation de CA Client Automation qui ne fonctionne pas !

Valeur par défaut : 0 (non)

DSM_LANGUAGE

Indique la langue de l'installation. Les valeurs possibles sont enu (anglais (U.S)) deu (allemand), fra (français) et jpn (japonais). Même si la valeur de propriété n'est pas enu, les fichiers de l'installation enu sont toujours installés en plus des fichiers de la langue spécifiée.

Par défaut : Vide (NULL) Cela force le programme d'installation à utiliser l'environnement linguistique par défaut. Si l'environnement linguistique par défaut du système ne figure pas parmi les environnements pris en charge, enu (anglais) est utilisé.

Remarque : DSM_LANGUAGE n'indique par la langue des boîtes de dialogue de l'assistant d'installation.

ITRM_AUTOSTART_INSTALL

Indique si les démons DSM doivent être démarrés après l'installation. Indiquez 0 pour empêcher le démarrage des démons DSM après l'installation.

Valeur par défaut : 1 (oui)

ITRM_AUTOSTART_REBOOT

Indique si les démons DSM doivent être démarrés au redémarrage de l'hôte. Indiquez 0 pour que les démons DSM ne démarrent pas automatiquement.

Valeur par défaut : 1 (oui)

ITRM_INST_CMDLINE

Spécifie si les utilitaires de ligne de commande software delivery et automated deployment (DMSweep) doivent être installés. Indiquez 0 pour ne pas installer ces utilitaires.

Valeur par défaut : 1 (oui)

ITRM_SETUP_SYS_PROFILE

Indique si le profil système (/etc/profile ou équivalent) doit être modifié pour configurer l'environnement DSM pour tous les utilisateurs de connexion. Spécifiez la valeur 0 pour laisser le profil du système inchangé.

Valeur par défaut : 1 (oui)

FIPS_MODE

Spécifie le mode FIPS de Client Automation. Entrez 1 pour activer le mode Préférence FIPS et 2 pour le mode FIPS uniquement.

Mode par défaut : 1 (Préférence FIPS)

Propriétés générales de l'agent

ITRM_INST_AGENT

Spécifie si des agents DSM doivent être installés. Si cette propriété n'est pas définie, aucune fonction d'agent n'est installée sauf si d'autres fonctions en dépendent. Indiquez 0 pour ne pas déployer de fonctions d'agent sauf si d'autres paramètres l'exigent.

Valeur par défaut : 1 (oui)

ITRM_SERVER

Spécifie le nom de l'hôte du serveur de modularité auquel l'agent DSM se connecte. Ce paramètre est utilisé uniquement si $ITRM_INST_AGENT est défini sur 1.

Valeur par défaut : *Nom d'hôte local*

ITRM_AGENT_DEFAULTGROUPS

Spécifie les groupes de gestion que l'agent doit rejoindre, dans une liste séparée par des virgules sans espaces.

Valeur par défaut : Null (ce qui signifie que l'agent ne rejoint aucun groupe)

Propriétés générales du serveur de modularité (Linux uniquement)

ITRM_INST_SERVER

Spécifie si un serveur de modularité DSM doit être installé. Si elle n'est pas définie, aucune fonction de serveur de modularité n'est installée. Ce paramètre est ignoré pour les packages d'agent uniquement. Indiquez 0 pour ne pas installer de serveur de modularité.

Valeur par défaut : 1 (oui)

ITRM_MANAGER

Spécifie le nom de l'hôte du gestionnaire de domaine auquel le serveur de modularité DSM envoie ses rapports. Ce paramètre est utilisé uniquement si $ITRM_INST_SERVER est défini sur 1.

Valeur par défaut : *Nom d'hôte local*

Propriétés du serveur de modularité (Linux uniquement)

ITRM_ENGINE

Spécifie le nom du moteur utilisé par le serveur de modularité. Une valeur vide indique le moteur du système.

Par défaut : Null

ITRM_PATH_COMMON_SERVER_DB

Spécifie le chemin du répertoire de la base de données du serveur de modularité.

Valeur par défaut : $CA_DSM_CONFIGDATA/Server/serverdb

Propriétés de l'agent Asset Management

ITRM_INST_AM_AGENT

Spécifie si l'agent Asset Management (AM) doit être installé. Indiquez 0 pour ne pas installer cet agent.

Valeur par défaut : 1 (oui)

ITRM_AMAGENT_CMDFILE_USER

Spécifie l'ID utilisateur sous lequel l'agent AM exécute un fichier de commande.

Par défaut : root

ITRM_AMAGENT_EXTUTILITY_USER

Spécifie l'ID utilisateur sous lequel l'agent AM exécute un utilitaire.

Par défaut : root

ITRM_AMAGENT_DMSCRIPT_USER

Spécifie l'ID utilisateur sous lequel l'agent AM exécute un DMScript.

Par défaut : root

ITRM_AMAGENT_USER_INVENTORY

Spécifie si le module user inventory doit être installé. Indiquez 0 pour ne pas installer le module user inventory.

Valeur par défaut : 1 (oui)

ITRM_AMAGENT_WITHCRONINFO

Spécifie si des informations crontab doivent être affichées. Indiquez 0 pour ne pas afficher d'informations.

Valeur par défaut : 1 (oui)

ITRM_AMAGENT_WITHUSERINFO

Spécifie si des informations sur l'utilisateur doivent être affichées. Indiquez 0 pour ne pas afficher d'informations.

Valeur par défaut : 1 (oui)

ITRM_AMAGENT_PRIO_LEVEL

Incrémente la priorité du processus de gestion des actifs. La plage de priorité est comprise entre -20 et 19.

Valeur par défaut : 0

ITRM_AMAGENT_EXACTINTERVAL

Spécifie si l'agent AM doit être exécuté par intervalles (valeur = 1) ou à heures fixes (valeur = 0).

Valeur par défaut : 1

ITRM_AMAGENT_RANDOM

Spécifie si l'agent AM doit être exécuté pendant un intervalle spécifique (valeur = 0) ou pendant un intervalle choisi de manière aléatoire (valeur = 1). Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=1.

Valeur par défaut : 0

ITRM_AMAGENT_WEEKLY

Spécifie que l'agent AM doit être exécuté toutes les n semaines. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=1.

Valeur par défaut : 0

ITRM_AMAGENT_DAILY

Spécifie que l'agent AM doit être exécuté tous les n jours. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=1.

Valeur par défaut : 1

ITRM_AMAGENT_HOURLY

Spécifie que l'agent AM doit être exécuté toutes les n heures. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=1.

Valeur par défaut : 0

ITRM_AMAGENT_EXMONDAY

Indique que l'agent AM ne doit pas être exécuté le lundi, si la valeur = 1. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 0 (l'agent est exécuté le lundi)

ITRM_AMAGENT_EXTUESDAY

Indique que l'agent AM ne doit pas être exécuté le mardi, si la valeur = 1. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 0 (l'agent est exécuté le mardi)

ITRM_AMAGENT_EXWEDNESDAY

Indique que l'agent AM ne doit pas être exécuté le mercredi, si la valeur = 1. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 0 (l'agent est exécuté le mercredi)

ITRM_AMAGENT_EXTHURSDAY

Indique que l'agent AM ne doit pas être exécuté le jeudi, si la valeur = 1. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 0 (l'agent est exécuté le jeudi)

ITRM_AMAGENT_EXFRIDAY

Indique que l'agent AM ne doit pas être exécuté le vendredi, si la valeur = 1. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 0 (l'agent est exécuté le vendredi)

ITRM_AMAGENT_EXSATURDAY

Indique que l'agent AM ne doit pas être exécuté le samedi, si la valeur = 1. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 0 (l'agent est exécuté le samedi)

ITRM_AMAGENT_EXSUNDAY

Indique que l'agent AM ne doit pas être exécuté le dimanche, si la valeur = 1. Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 0 (l'agent est exécuté le dimanche)

ITRM_AMAGENT_EXECUTETIME

Spécifie que l'exécution de l'agent AM doit commencer à cette heure de la journée. L'heure a la format hh:mm (heure:minute). Ce paramètre est utile uniquement si $ITRM_AMAGENT_EXACTINTERVAL=0.

Valeur par défaut : 00:00 (minuit)

Propriétés générales d'Asset Management

ITRM_INST_AM

Spécifie si le composant Asset Management (AM) doit être installé. Si elle n'est pas définie, aucune fonction AM n'est installée. Indiquez 0 pour ne pas installer de fonctions AM.

Valeur par défaut : 1 (oui)

Propriétés du serveur de modularité d'utilisation de logiciels Asset Management (Linux uniquement)

ITRM_INST_AM_METER_SERVER

Spécifie si le serveur de modularité d'utilisation de logiciels Asset Management (AM) doit être installé. Spécifiez 0 pour ne pas installer de serveur de modularité d'utilisation de logiciels.

Valeur par défaut : 1 (oui)

Propriétés du serveur de secteur Asset Management (Linux uniquement)

ITRM_INST_AM_SECTOR_SERVER

Spécifie si le serveur de secteur Asset Management (AM) doit être installé. Indiquez 0 pour ne pas installer le serveur de secteur.

Valeur par défaut : 1 (oui)

Propriétés DMPrimer

ITRM_INST_DMPRIMER

Spécifie si DMPrimer doit être installé. Indiquez 0 pour ne pas installer le DMPrimer.

Valeur par défaut : 1 (oui)

Propriétés générales du service de transport de données (Solaris uniquement)

DTS_PPP_USER

(Utilisé sur Solaris uniquement) Spécifie si un utilisateur PPP doit être créé. Ce paramètre est ignoré si les protocoles asppp ou Solstice PPP ne sont pas détectés. Indiquez 1 pour créer un utilisateur PPP.

Valeur par défaut : 0 (non)

Propriétés générales de RC (Linux/Mac OS X uniquement)

ITRM_INST_RC

Spécifie si des composants Remote Control doivent être installés. Si elle n'est pas définie, aucune fonction Remote Control n'est installée. Indiquez la valeur 0 pour ne pas installer de composants Remote Control.

Valeur par défaut : 1 (oui)

Propriétés de l'agent Remote Control (Linux/Mac OS X uniquement)

ITRM_INST_RC_AGENT

Spécifie si l'agent Remote Control doit être installé. Indiquez 0 pour ne pas installer l'agent.

Valeur par défaut : 1 (oui)

ITRM_RC_AGENT_STANDALONE

Spécifie si l'agent Remote Control est géré de manière centralisée (valeur = 0) ou autonome (valeur = 1).

Valeur par défaut : 0

ITRM_RC_AGENT_IN_MGMT_GROUPS

Spécifie si un agent géré va apparaître dans les groupes de gestion.

Valeur par défaut : 1 (oui)

Propriétés du serveur de modularité Remote Control (Linux uniquement)

ITRM_INST_RC_SERVER

Spécifie s'il faut installer le composant du serveur de modularité Remote Control. Indiquez 0 pour ne pas installer de serveur de modularité Remote Control.

Valeur par défaut : 1 (oui)

Propriétés générales de Software Delivery

ITRM_INST_SD

Spécifie si des composants software delivery doivent être installés. Si ce n'est pas le cas, aucune fonction Software Delivery n'est installée. Indiquez 0 pour ne pas installer de composants Software Delivery.

Valeur par défaut : 1 (oui)

Propriétés de l'agent Software Delivery

ITRM_INST_SD_AGENT

Spécifie si l'agent Software Delivery (SD) doit être installé. Indiquez 0 pour ne pas installer l'agent.

Valeur par défaut : 1 (oui)

CA_DSM_REPLACE_PRE_R11_SD_AGENT

Spécifie si l'agent antérieur à la version r11 de SD doit être remplacé (c.-à-d. supprimé) ou doit permettre une co-existence. Utile uniquement si un agent SD antérieur à r11est déjà installé sur le système. Indiquez 1 pour entraîner la suppression des agents antérieurs.

Valeur par défaut : 0 (co-existence).

Propriétés du serveur de démarrage SD (Linux uniquement)

FIPS_MODE

Indique le mode FIPS défini par le programme d'installation de Client Automation. Les valeurs valides sont 1 (Préférence FIPS) et 2 (FIPS uniquement).

ITRM_INST_SD_BOOTSERVER

Spécifie si le serveur de démarrage Software Delivery (SD) doit être installé. En général, les serveurs de modularité et les serveurs de démarrage sont installés sur le même hôte. Spécifiez 0 pour ne pas installer de serveur de démarrage.

Valeur par défaut : 1 (oui)

ITRM_BOOTSERVER_OS_INSTALL_PATH

Spécifie l'emplacement de la bibliothèque d'images du système d'exploitation OSIM.

Valeur par défaut : $ITRM_PATH_COMMON_SERVER_DB/SDBS/var

BOOTSERVER_ENABLED

Détermine l'activation ou non du service Serveur de démarrage. Indiquez 0 pour désactiver le service.

Valeur par défaut : 1 (oui)

BOOTSERVER_DISABLESHARES

Spécifie s'il faut désactiver ou non les partages SMB. Spécifiez 0 pour activer les partages SMB.

Valeur par défaut : 1 (oui)

Propriétés du serveur de modularité SD (Linux uniquement)

ITRM_INST_SD_STAGSERVER

Spécifie si le composant du serveur de modularité Software Delivery (SD) doit être installé. En général, les serveurs de modularité et les serveurs de démarrage sont installés sur le même hôte. Indiquez 0 pour ne pas installer un serveur de modularité SD.

Valeur par défaut : 1 (oui)

SDLIBRARY

Spécifie l'emplacement de la bibliothèque de packages logiciels.

Valeur par défaut : $CA_DSM_CONFIGDATA/sd/asm/library

ITRM_SD_EXPORT_NFS_SHARE

Spécifie s'il faut exporter $SDLIBRARY en tant que partage NFS. Spécifiez 1 pour exporter $SDLIBRARY.

Valeur par défaut : 0 (non)

ITRM_SD_EXPORT_SAMBA_SHARE

Spécifie s'il faut exporter $SDLIBRARY en tant que partage SAMBA. Spécifiez 1 pour l'exporter en tant que partage SAMBA.

Valeur par défaut : 0 (non)

DSM_SD_INSTALL_CCS_CALENDAR

Spécifie si l'utilisation du calendrier CCS doit être installée (gestion d'événements). Disponible uniquement si la distribution CCS l'est également ou est déjà installée. Spécifiez 1 pour installer l'utilisation du calendrier CCS.

Valeur par défaut : 0 (non)

Propriétés de la console Web (Linux uniquement)

ITRM_INST_WEBGUI

Spécifie s'il faut installer ou non la console Web. Spécifiez 1 pour installer la console Web.

Valeur par défaut : 0 (non)

Propriétés des services Web (Linux uniquement)

ITRM_INST_WEBSERVICES

Spécifie s'il faut installer ou non les services Web. Spécifiez 1 pour installer les services Web.

Valeur par défaut : 0 (non)

WAC_MANAGER

Spécifie le gestionnaire auquel se connectent les services Web.

Valeur par défaut : *Nom d'hôte local*

DSM_TOMCAT_PORT

Spécifie le port TCP/IP où le gestionnaire écoute les demandes.

Valeur par défaut : 8090

DSM_TOMCAT_SHUT

Spécifie le port TCP/IP où le gestionnaire écoute les demandes d'arrêt.

Valeur par défaut : 8095

DSM_TOMCAT_AJP

Spécifie le port sur lequel le travail écoute les demandes Ajp13, afin de les transmettre aux travaux hors processus à l'aide du protocole Ajpv13.

Valeur par défaut : 8020

ITRM_AMS_WEBPORT

Spécifie le port Web du système de maintenance des actifs.

Valeur par défaut : 8080

Propriétés de l'outil de packaging PIF

ITRM_INST_PACKAGER

Spécifie s'il faut installer ou non le kit de développement logiciel (SDK) du produit PIF. Le SDK peut être installé seul, indépendamment de Client Automation. Spécifiez 0 pour ne pas installer le SDK.

Valeur par défaut : 1 (oui)

Propriétés de la documentation (Linux uniquement)

ITRM_INST_DOC

Spécifie s'il faut installer ou non la documentation. Spécifiez 0 pour ne pas installer la documentation.

Valeur par défaut : 1 (oui)

Fichiers journaux d'installation

Toute activité du programme d'installation CA Client Automation est consignée dans des fichiers automatiquement créés par le programme d'installation.

CA Technologies fournit un outil de collection de fichier journal, dsminfo, vous permettant de relever toutes les informations dont vous avez besoin pour analyser un problème éventuel avec Client Automation.

L'outil dsminfo est disponible sur le support en ligne CA et peut être téléchargé sur : http://www.ca.com/worldwide.

Fichiers journaux d'installation sous Windows

Le programme d'installation crée les types de fichiers journaux suivants sous Windows :

DSMSetupxxx.log

Créé par Microsoft Windows Installer (MSI) et enregistré dans le répertoire spécifié par la variable d'environnement %temp%. Ce fichier journal est créé lors de l'utilisation du gestionnaire, du serveur de modularité, de l'explorateur DSM et des agents. Chaque package MSI crée un fichier journal distinct.

TRC_*xxx*.log

Créé par des processus internes et enregistré dans le répertoire spécifié par la variable d'environnement %temp%. Ces fichiers indiquent la configuration des composants installés, par exemple la configuration de CAF, du gestionnaire ou de la base de données.

Dans les noms de fichier journal, la chaîne *xxx* est remplacée par le nom du composant auquel appartiennent les informations du journal, par exemple DSMSetupManager.log.

Fichiers journaux d'installation sous Linux et UNIX

Le fichier journal d'installation initiale sous Linux et UNIX s'appelle ca-dsm.install.log. Si vous modifiez l'installation, le fichier journal s'appelle ca-dsm.reinstall.log. Lorsque vous supprimez le produit, le fichier journal devient ca-dsm.deinstall.log.

Sous Linux et UNIX, les fichiers journaux d'installation sont enregistrés dans les répertoires suivants :

- /tmp
- /opt/CA/installer/log

Informations relatives à la version des Composants DSM installés

Le programme d'installation fournit des informations relatives à la version des composants et fonctions CA Client Automation installés. Vous pouvez également accéder à ces informations via la commande dsmver.

Les informations relatives à la version s'affichent au format M.m.b.r, où M = numéro de version principale, m = numéro de version mineure, b = numéro de sous-version et r = numéro de version/patch. Par exemple, pour la version 12.0.01234.1, la version principale est 12, la version mineure 0, la sous-version 1234 et la révision 1.

Pour afficher les composants et fonctions installés ainsi que leur version, saisissez la commande dsmver dans la ligne de commande.

La commande dsmver a le format suivant :

```
dsmver
```

Le format de sortie des informations relatives à la version est indiqué dans l'exemple suivant :

```
Desktop and Server Management
-------------------------------------------
Explorateur - Asset Management        12.0.1234.1
Explorateur - Remote Control          12.0.1234.1
Explorateur - Software Delivery       12.0.1234.1
Gestionnaire - Moteur                   12.0.1234.1
Gestionnaire - Asset Management        12.0.1234.1
Gestionnaire - Data Transport           12.0.1234.1
Serveur
. . . . .
```

Chapitre 4: Tâches post-installation

Ce chapitre fournit des informations relatives à la modification, la réparation, la mise à niveau et la désinstallation d'une installation existante.

Ce chapitre traite des sujets suivants :

Modification de la langue du produit après l'installation

La liste ci-dessous contient des informations utiles sur le changement de la langue d'CA Client Automation après l'installation :

- Il existe plusieurs méthodes pour modifier la langue du produit après l'installation.
  - La modification de la langue des composants DSM installés est prise en charge pour les composants de l'explorateur, du serveur de modularité et des agents. Sur l'hôte agent, exécutez la commande ccnfcmda comme suit :

    ```
    ccnfcmda -cmd SetParameterValue -ps itrm/common/localization
    -pn language -v langue
    ```

    La valeur de *langue* indique la langue souhaitée. Les valeurs possibles sont enu (anglais (Etats-Unis)), deu (allemand), fra (français) et jpn (japonais) ; pour les agents, viennent s'ajouter chs (chinois simplifié), esn (espagnol) et kor (coréen).

    Remarque : Pour plus d'informations sur la commande ccnfcmda de l'agent de configuration, saisissez <command> / ? dans l'invite de commande.
  - Créez une stratégie utilisant un système de requête pour exécuter la commande ccnfcmda comme décrit ci-dessus.
- Notez que la modification de la langue du gestionnaire est impossible une fois ce dernier installé.

- Lorsque vous configurez la langue de CA Client Automation, vérifiez que le package linguistique correspondant à la langue spécifiée a été installé car aucune vérification de disponibilité n'est effectuée. Si aucun package linguistique correspondant à la langue souhaitée n'a été installé, CA Client Automation repasse alors en anglais (Etats-Unis).
- Lorsque la langue est reconfigurée, vous devez arrêter et redémarrer CA Client Automation à l'aide des commandes caf stop et cafstart respectivement, afin que la nouvelle valeur soit prise en compte.

Informations complémentaires :

Installation multilingue (page 123)

Maintenance de la MDB

Les paragraphes qui suivent indiquent comment maintenir et synchroniser la base de données de gestion (MDB).

Maintenance de la MDB Microsoft SQL Server

Les tables de base de données Microsoft SQL Server (SQL Server) doivent être optimisées à chaque mise à jour de la base de données avec une quantité de données significative.

Pour vous aider à administrer la base de données de gestion (MDB) dans SQL Server, CA Client Automation fournit le script de maintenance DsmMSSqlOpt.bat que les administrateurs peuvent appliquer régulièrement.

Le script DsmMSSqlOpt.bat vous aide à optimiser les tables de base de données en effectuant des tâches de maintenance telles que la défragmentation de l'index et la mise à jour des statistiques. Le script concerne uniquement les tables appartenant à CA Client Automation.

Le script de maintenance DsmMSSqlOpt.bat est automatiquement installé à l'emplacement suivant lors de l'installation de CA Client Automation :

```
%Program Files$\CA\DSM\database\mdb_install\mssql\DsmMsSqlOpt.bat
```

Le script de maintenance DsmMSSqlOpt.bat est également disponible sur le support d'installation (DVD) de CA Client Automation, à l'emplacement suivant :

```
Maintenance\Windows\mssql\DsmMsSqlOpt.bat
```

Le script de maintenance DsmMSSqlOpt.bat peut être exécuté avec certaines options de la manière suivante :

```
DsmMsSqlOpt.bat [-pagecount=n] [-maxfrag=m] [ -usereindex] [ {local | NomServeur} [NomMDB] ]
```

-pagecount

Spécifie le nombre maximum *n* de pages pour les tables ou les index. Les tables ou index comportant un nombre de pages supérieur à celui spécifié sont défragmentés. *n* est une valeur numérique.

Valeur par défaut : 1000

-maxfrag

Spécifie un degré *m* de fragmentation. Les tables comportant le degré de fragmentation spécifié seront défragmentées. *m* est une valeur numérique.

Valeur par défaut : 10

-usereindex

Spécifie que les index doivent être reconstruits et non pas défragmentés. Par défaut, le script DsmMsSqlOpt effectue une défragmentation des index.

Si vous possédez un gestionnaire d'entreprise DSM en plus des gestionnaires de domaines, rappelez-vous que le script de maintenance doit être exécuté sur les bases de données des deux niveaux. Nous vous recommandons d'exécuter le script au moins une fois après que les 1 000 premiers actifs informatiques aient été enregistrés dans la base de données du domaine. Ensuite, le script doit être exécuté à chaque inscription de 5 000 actifs d'ordinateur supplémentaires. Dans le gestionnaire d'entreprise, la maintenance doit être effectuée chaque fois que 5 000 actifs informatiques ont été dupliqués à partir des gestionnaires de domaines associés.

Le script DsmMsSqlOpt.bat doit être exécuté localement sur l'ordinateur où est installée la base de données de gestion (MDB). Ce script propose deux options : il peut servir à reconstruire des index ou à défragmenter des index. Avant d'exécuter le script avec l'option de reconstruction, nous vous recommandons d'éteindre les composants du gestionnaire qui accèdent à la MDB. Ces composants de DSM doivent être redémarrés une fois l'exécution du script terminée.

Une fois le script appelé à l'aide de l'option qui sert à défragmenter les index, les composants DSM peuvent être conservés et exécutés. Cependant, les opérations initiées par le script demandent beaucoup de ressources et risquent d'avoir un impact négatif sur les performances. En outre, sachez que pour des bases de données importantes, la défragmentation des index peut nécessiter plusieurs heures.

Par conséquent, vous devez planifier les tâches de maintenance de MDB à des moments où la charge de travail sur ces MDB est réduite, voire inexistante. Par exemple, vous pouvez planifier le script afin qu'il soit exécuté une fois par semaine durant la nuit ou pendant les week-ends.

Remarques importantes concernant la maintenance de la MDB SQL Server

Ci-dessous figurent quelques remarques sur la maintenance de la MDB Microsoft SQL Server :

- La variable %TEMP% doit être définie pour un répertoire de travail approprié avant l'exécution du script DsmMsSqlOpt.bat.
- Il convient de reconstruire les index dont le degré de fragmentation excède 30% lors de la première étape de maintenance, car l'exécution de la reconstruction d'index est beaucoup plus rapide que celle de la défragmentation. Pour cela, vous devez exécuter le script DsmMsSqlOpt à l'aide des options -usereindex et -maxfrag=30, par exemple :

  ```
  DsmMsSqlOpt.bat -maxfrag=30 -usereindex
  ```
- Après l'étape initiale, toutes les tables dont la défragmentation est inférieure à 10% doivent être défragmentées. Pour cela, vous pouvez appeler le script DsmMsSqlOpt avec cette option -maxfrag=10, par exemple :

  ```
  DsmMsSqlOpt.bat -maxfrag=10
  ```

Maintenance de la MDB Oracle

Pour résoudre les problèmes liés aux performances avec la MDB Oracle, effectuez l'une des opérations suivantes :

- A partir d'un outil Oracle SQL sur l'ordinateur Solaris équipé du serveur Oracle, exécutez la commande suivante :

  ```
  EXEC DBMS_STATS.gather_schema_stats(ownname =>'MDBADMIN', cascade =>true,
  method_opt=>'FOR ALL COLUMNS SIZE AUTO');
  ```
- Connectez-vous à l'ordinateur Solaris à l'aide des informations d'identification de l'utilisateur d'Oracle, puis, dans l'interface de commande, exécutez la commande indiquée dans l'exemple suivant :

  ```
  echo "EXEC DBMS_STATS.gather_schema_stats (ownname => 'MDBADMIN', cascade
  =>true, method_opt=>'FOR ALL COLUMNS SIZE AUTO');"|sqlplus
  sys/<mot_de_passe>@<instance> as sysdba
  ```

  Dans cet exemple, <*mot_de_passe*> correspond au mot de passe de l'instance Oracle actuelle et <*instance*> au nom de l'instance Oracle actuelle (SID).

Informations complémentaires :

Installation d'une MDB Oracle distante (page 144)

Objets synchronisés vers la MDB cible

Les objets qui sont synchronisés vers les MDB cibles basées sur SQL Server et Oracle comprennent les types suivants :

- **Actifs primaires et informations sur l'utilisateur**
  - Ordinateurs détectés
  - Utilisateurs détectés
  - Utilisateurs d'ordinateurs détectés (relations entre ordinateurs et utilisateurs)
- **Inventaire matériel**
  - Inventaire général des ordinateurs
- **Inventaire logiciel**
  - Signatures logicielles
  - Inventaire logiciel des ordinateurs (inventaire logiciel basé sur la signature et heuristique)

Création de la tâche de synchronisation

La synchronisation des actifs DSM et des données d'inventaire à l'aide d'une MDB cible basée sur SQL Server ou Oracle est initiée par une tâche de moteur exécutée à un moment planifié. Vous créez cette tâche et définissez sa planification via l'IUG de l'explorateur DSM.

La tâche de moteur qui effectue la synchronisation des actifs DSM et des données d'inventaire à l'aide d'une MDB existant sur Microsoft SQL Server est créée, configurée, attribuée, planifiée et exécutée de la même manière que toutes les autres tâches de moteur DSM. Accédez à Panneau de configuration, Moteurs, Tous les moteurs dans l'explorateur DSM et cliquez avec le bouton droit sur le moteur qui doit exécuter la tâche de synchronisation, puis sélectionnez Ajouter une nouvelle tâche dans le menu contextuel. L'assistant Ajouter une nouvelle tâche s'ouvre et vous guide tout au long de la création de la tâche de synchronisation.

Dans l'assistant Créer une nouvelle tâche, vous parcourez les étapes suivantes :

- Sur la première page de l'assistant, sélectionnez le type de tâche Synchronisation de la base de données à partir de la liste déroulante Type de tâche.
- Sur la deuxième page de l'assistant, saisissez un nom et une description adaptés à la tâche de synchronisation de la base de données qui reflètent l'objectif et le type de la tâche.

- Sur la troisième page de l'assistant, indiquez le type de base de données cible et les informations d'identification pour la MDB cible, comme décrit dans la section Options de configuration de la tâche de synchronisation (page 222). Vous pouvez immédiatement tester vos paramètres en cliquant sur le bouton Tester la connexion. Avant de quitter cette page, l'assistant vérifie que la MDB cible existe et satisfait aux conditions requises.
- Sur la quatrième page de l'assistant, cliquez sur le bouton Définir la planification si vous souhaitez modifier la planification prédéfinie pour la tâche de synchronisation, qui est "Généralement programmé pour être toujours exécuté". Cliquez sur Terminer pour utiliser la planification prédéfinie et fermer l'assistant.

Synchronisation des options de configuration des tâches

Pendant la création de la tâche de synchronisation, vous devez spécifier les informations d'identification (propriétés de connexion) pour la MDB cible sur l'une des pages de l'assistant Créer une nouvelle tâche.

- **MDB cible basée sur SQL Server :**

  Pour une MDB cible basée sur SQL Server, les informations d'identification requises comprennent :

  - Type de serveur de la MDB cible (valeur : serveur MS SQL)
  - Nom de l'ordinateur hébergeant la MDB cible
  - Instance du serveur de la base de données et numéro de port (par défaut : <aucune>)
  - Nom de la base de données
  - Nom d'utilisateur sur la MDB cible

    Le nom d'utilisateur est ca_itrm et ne peut être modifié.
  - Mot de passe sur la MDB cible

    Important : Ici, vous devez entrer le mot de passe que vous avez spécifié à l'aide du paramètre de mot de passe CA_ITRM dans la configuration de Client Automation lors de la mise à niveau de la MDB de SQL Server pour synchronisation.

- **MDB cible basée sur Oracle :**

  Pour une MDB cible basée sur Oracle, les informations d'identification requises comprennent :

  - Type de serveur de la MDB cible (valeur : Oracle)
  - Nom de l'ordinateur hébergeant la MDB cible
  - ID du serveur de la MDB cible (par défaut : orcl)
  - Numéro de port pour la MDB cible Oracle (par défaut : 1521)
  - Nom d'utilisateur sur la MDB cible

    Le nom d'utilisateur est ca_itrm et ne peut être modifié.

  - Mot de passe sur la MDB cible

    Important : Ici, vous devez entrer le mot de passe que vous avez spécifié à l'aide du paramètre de mot de passe CA_ITRM dans le programme d'installation de MDB de Client Automation lors de la mise à niveau de la MDB de Oracle sur Solaris pour synchronisation.

Vous pouvez tester immédiatement les paramètres saisis en cliquant sur le bouton Tester la connexion, sur la même page de l'assistant. Le gestionnaire essaie alors d'ouvrir une connexion vers la MDB cible. Le résultat de cette action s'affiche à côté du bouton Tester la connexion (par exemple : Réussite de la connexion).

Vous pouvez configurer la planification pour la tâche de synchronisation en cliquant sur le bouton Configurer la planification sur la page Planification de l'assistant Créer une nouvelle tâche. La configuration par défaut est "Généralement programmé de façon à être exécuté en permanence".

Options et restrictions de la synchronisation

Vous disposez des options suivantes pour exécuter la tâche de synchronisation :

- Synchronisation des données à partir de la MDB sur le gestionnaire de domaine DSM vers la MDB cible.
- Synchronisation des données à partir de la MDB sur le gestionnaire d'entreprise DSM vers la MDB cible. Cela inclut la synchronisation des données de tous les gestionnaires de domaine rapportées au gestionnaire d'entreprise.

Les restrictions suivantes s'appliquent à la synchronisation :

- Vous ne devez pas synchroniser des données à partir de la MDB d'un gestionnaire de domaine DSM lorsque le gestionnaire d'entreprise associé synchronise déjà la même MDB cible. Si vous procédez ainsi, cela engendrera un chargement de données inutile sur le réseau.
- Vous ne devez pas synchroniser les données à partir d'une MDB du gestionnaire d'entreprise DSM lorsque l'un de ses gestionnaires de domaine associés synchronise déjà la même MDB cible. Si vous procédez ainsi, cela engendrera une charge de données inutile sur le réseau.

Suppression de la synchronisation

Si vous souhaitez supprimer la synchronisation entre la MDB source SQL Server Microsoft et la MDB cible, vous devez supprimer la tâche de synchronisation.

Vous commencez la suppression de la tâche de synchronisation depuis le répertoire Toutes les tâches de moteur sur l'IU de l'explorateur DSM tandis que la tâche de synchronisation est liée à un moteur. Cliquez avec le bouton droit de la souris sur la tâche du moteur, puis sélectionnez Supprimer dans le menu contextuel. Vous devrez confirmer la suppression de l'élément sélectionné.

Cependant, la tâche de synchronisation n'est pas immédiatement supprimée. La boîte de dialogue Supprimer la tâche vous avertit que le moteur doit être exécuté une fois de plus avant que la tâche de synchronisation ne soit supprimée.

Dans la boîte de dialogue Supprimer la tâche, vous pouvez également sélectionner que le moteur nettoie la MDB cible en ce qui concerne les objets synchronisés. Si vous ne sélectionnez pas cette option, le moteur nettoie uniquement la MDB source. Si vous sélectionnez cette option, l'état de la tâche de synchronisation passe à "En attente de nettoyage de la base de données de la part du moteur". Une fois la tâche de nettoyage réalisée par le moteur la fois suivante prévue, le moteur délie et supprime la tâche de synchronisation.

Désinstallation du gestionnaire DSM et de la MDB

Lors de la désinstallation du gestionnaire DSM, la MDB n'est pas désinstallée et reste sur le système.

La MDB est utilisée par plusieurs produits CA Technologies pouvant être installés localement avec la MDB ou pouvant l'utiliser à distance. La désinstallation de l'un de ces produits CA Technologies ne signifie pas nécessairement que la MDB n'est plus utilisée.

Nous vous recommandons de laisser un administrateur autorisé désinstaller la MDB et le fournisseur MDB sélectionné après un examen attentif de toutes les conséquences sur l'utilisation locale ou distante par d'autres produits CA Technologies.

Une MDB Microsoft SQL Server peut être supprimée à l'aide du gestionnaire d'entreprise Microsoft SQL qui permet la sélection et la suppression de la base de données MDB. SQL Server Management Studio est un autre outil pouvant être utilisé pour supprimer une MDB MS SQL Server.

Pour supprimer une MDB Oracle, sélectionnez Désinstaller dans le programme d'installation, ce qui supprimera la partie correspondant au produit PIF dans le schéma de la MDB. Ensuite, en ouvrant une session sous le nom 'oracle', vous pourrez utiliser l'outil d'administration d'Oracle dbca pour supprimer les tables de la base de données. Enfin, vous pourrez supprimer vous-même tous les fichiers restés dans le dossier ../opt/CA/SharedComponents/oracle/mdb en ouvrant une session sous le nom 'root'.

Remarque : Pour plus d'informations sur la suppression d'une MDB Oracle, consultez le document *Présentation de la MDB* dans la documentation Client Automation (Bibliothèque) ou la documentation Oracle correspondante.

Si vous désinstallez un gestionnaire DSM, vous devez supprimer manuellement l'utilisateur ca_itrm de Microsoft SQL Server, ainsi que le compte ca_itrm_ams le cas échéant. La réinstallation de Client Automation avec le serveur Microsoft SQL Server peut ne pas fonctionner si l'utilisateur ca_itrm figure toujours dans ce serveur. Si CCS a été utilisé et est déjà désinstallé, les comptes ndsadmin et hostname\TNDUsers devront également être supprimés de SQL Server.

Si vous désinstallez un gestionnaire DSM, les données correspondantes contenues dans la MDB ne sont pas supprimées par défaut.

L'assistant d'installation Client Automation offre une fonctionnalité permettant de supprimer des données de la MDB.

Si, pour une raison quelconque, vous ne voulez pas utiliser cette méthode de suppression de données de la MDB, vous devez exécuter le script data_uninstall (page 227) afin de nettoyer la MDB. Ce script prend en charge Microsoft SQL Server et Oracle. Les versions appropriées du script, data_uninstall.bat (pour SQL Server) et data_uninstall.sh (pour Oracle) sont disponibles aux emplacements suivants sur le DVD d'installation de Client Automation :

- *dvdroot*\Maintenance\Windows\mssql\
- *dvdroot*\Maintenance\Windows\oracle\

Copiez tous les fichiers à partir du répertoire respectif sur votre système gestionnaire local, puis exécutez le script data_uninstall avec les paramètres appropriés à partir de l'invite de commande.

Voici une liste de scénarios qui expliquent l'utilisation du script data_uninstall :

Supprimer définitivement le gestionnaire

Si Client Automation était la seule application, vous pouvez supprimer la MDB manuellement.

Sinon, exécutez le script data_uninstall et configurez les indicateurs pour -pdata d et -data d.

Nettoyage du gestionnaire pour un nouveau démarrage

Si Client Automation était la seule application, vous pouvez supprimer la MDB manuellement.

Sinon, exécutez le script data_uninstall et configurez les indicateurs pour -pdata d et -cdata d.

Si vous souhaitez également supprimer les actifs enregistrés, vous devez définir l'argument -asset d.

Supprimer le gestionnaire mais conserver l'ensemble des données

Dans ce cas, certaines données au moins doivent être supprimées qui font référence à des objets de système de fichiers. Sinon, exécutez le script data_uninstall et configurez l'indicateur -sdonly. Cela supprime les références aux objets du système de fichiers Software Delivery associé, y compris les informations relatives au système de gestion des installations de systèmes d'exploitation (OSIM) et au démarrage.

Commande data_uninstall - Supprimer des données de la base de données

Utilisez la commande data_uninstall pour supprimer des données de la base de données ou vérifier des produits et des domaines enregistrés dans la base de données. La commande data_uninstall prend en charge Microsoft SQL Server et Oracle.

Cette commande possède différents formats :

```
data_uninstall -server nom_serveur
    -instance nom_instance:numéro_port
    -database nom_base_de_données
    -asset {k | d }
    -pdata {k | d }
    -cdata {k | d }
    -user
    -pwd
```

Supprime des données de la base de données, en fonction des indicateurs k ou d (k = conserver les données, d = supprimer les données) fournis avec les arguments. (Vous obtenez cette utilisation si vous exécutez la commande sans aucun argument).

```
data_uninstall -server nom_serveur
    -instance nom_instance:numéro_port
    -database nom_base_de_données
    -check
```

Imprime le nombre de produits enregistrés dans la MDB, ainsi que le nombre de domaines enregistrés dans la base de données.

```
data_uninstall -server nom_serveur
    -instance nom_instance:numéro_port
    -database nom_base_de_données
    -sdonly
```

Supprime uniquement les données Software Delivery en fonction de l'objet du système de fichier. Cette commande supprime également toutes les références MDB à OSIM et aux images de démarrage.

-server *nom_serveur*

Spécifie le nom du système SGBDR local.

Important : Le nom du serveur de base de données plus le nom de l'instance de base de données doivent comporter un maximum de 29 caractères.

-instance *nom_instance*:*numéro_port*

Identifie l'instance de la base de données, par exemple un nom d'instance Microsoft SQL Server. L'indication du numéro de port est obligatoire, sauf dans le cas de l'instance par défaut de Microsoft SQL Server. Dans le cas de l'instance Microsoft SQL Server par défaut, vous devez utiliser des guillemets pour définir un nom vide, -instance "", par exemple.

-database *nom_base_de_données*

Dans le cas de SQL Server, indique le nom de la base de données, par exemple mdb.

Dans le cas d'Oracle, indique la SID.

-asset {k|d}

Spécifie si l'enregistrement des données d'actif doit être annulé. Utilisez -asset k pour conserver les actifs, -asset d pour en annuler l'enregistrement.

-pdata {k|d}

Spécifie si les données propres au produit doivent être supprimées. Utilisez -pdata k pour conserver les données, -pdata d pour les supprimer.

-cdata {k|d}

Spécifie si les données communes Client Automation doivent être supprimées. Utilisez -cdata k pour conserver les données et -cdata d pour supprimer les données communes.

-user *nom_utilisateur*

Spécifie le nom d'utilisateur à utiliser pour se connecter à la base de données, par exemple ca_itrm.

-pwd:*mot_de_passe*

Spécifie le mot de passe de l'utilisateur indiqué à l'aide de -user.

-check

Vérifie si des produits CA Technologies sont encore enregistrés dans la base de données et répertorie tous les domaines enregistrés.

-sdonly

Supprime uniquement les données Software Delivery associées à des objets dans le système de fichiers, y compris OSIM et les données de démarrage.

Exemple : vérification des produits et des domaines

Cet exemple permet de vérifier simplement si des produits CA Technologies sont encore enregistrés dans la base de données MDB et répertorie tous les domaines enregistrés.

```
data_uninstall -server myMachine
    -instance ""
    -database mdb
    -check
```

Exemple : suppression de données à l'exception des actifs

Cet exemple illustre la suppression de toutes les données Client Automation de la base de données MDB, mais ne permet pas d'annuler l'enregistrement des actifs.

```
data_uninstall -server myMachine
    -instance ""
    -database mdb
    -check
    -asset k
    -pdata d
    -cdata d
    -user ca_itrm
    -pwd myPassword
```

Fichier journal data_uninstall

Après l'exécution du script data_uninstall, un fichier journal nommé data_uninstall.log figure dans le dossier Temporaire :

- Windows :
  `%TEMP%`
- Linux :
  `/tmp`

Installation de SQL Bridge

La fonctionnalité de synchronisation de SQL Bridge est installée dans votre environnement d'application dans le cadre de l'installation du gestionnaire DSM. Cela signifie que sur le côté source de SQL Bridge, aucune étape d'installation spéciale n'est nécessaire. Cependant, vous devez réaliser des opérations de mise à niveau sur le côté cible de SQL Bridge pour la MDB appropriée.

Mise à niveau côté cible avec une MDB Microsoft SQL Server 1.0.4

Microsoft SQL Server MDB 1.0.4 est utilisé avec Unicenter Asset Portfolio Management r11.3 sur Windows.

Pour mettre à niveau la MDB Microsoft SQL Server cible :

1. Exécutez le programme d'*installation de la MDB* à partir du DVD d'installation.

   Cette procédure applique tous les patchs MDB qui ne sont pas encore disponibles sur la MDB cible et créera l'utilisateur de la base de données ca_itrm.

2. Pour profiter pleinement de la caractéristique de synchronisation, vous devez télécharger et installer le correctif de test T5D6008 pour Windows, disponible auprès du support CA en ligne. Suivez les instructions d'installation détaillées fournies avec le correctif de test. T5D6008 inclut des correctifs applicables à Unicenter Asset Portfolio Management r11.3 sur Windows.

Mise à niveau côté cible avec une MDB Microsoft SQL Server 1.5

La MDB Microsoft SQL Server 1.5 est utilisée avec CA Service Desk Manager r12 sur Windows.

Pour mettre à niveau la MDB cible Microsoft SQL Server, exécutez le programme d'installation de la MDB à partir du DVD d'installation de Client Automation.

Cette procédure appliquera les dernières mises à jour des schémas de MDB pour DSM sur la MDB cible et créera l'utilisateur de la base de données ca_itrm.

Installation d'Oracle Bridge

La fonctionnalité de synchronisation d'Oracle Bridge est installée dans votre environnement d'application dans le cadre de l'installation du gestionnaire DSM. Cela signifie que sur le côté source de SQL Oracle, aucune étape d'installation spéciale n'est nécessaire. Cependant, vous devez réaliser des étapes de mise à niveau sur le côté cible de Oracle Bridge pour la MDB appropriée.

Mise à niveau côté cible avec la MDB Oracle 1.5 sous Solaris

La MDB Oracle 1.5 est utilisée avec CA Service Desk Manager r12 sur Windows.

Pour mettre à niveau la MDB Oracle cible :

1. Exécutez la configuration Programme d'installation de la MDB Oracle sur Solaris, qui est disponible sur le DVD d'installation de Client Automation Version 12.9.

   Cette procédure appliquera les dernières mises à jour des schémas de MDB pour DSM sur la MDB cible et créera l'utilisateur de la base de données ca_itrm.

2. Dans les fichiers AMS.Properties pour CA Service Desk Manager, ajoutez le nouveau paramètre de configuration :

   ```
   dsm_oracle_ddl=1
   ```

Exemple

L'exemple suivant montre l'apparence du fichier AMS.Properties :

```
Mot de passe de l'utilisateur # ca_itrm_ams pour se connecter à la base de
données du domaine DSM.
dsm_domain_db_password=
# Propriétaire de la table pour les tables créées à la volée pour DSM.
# Cette propriété ne doit jamais être définie si les tables
# n'ont pas été créées par ca_itrm.
dsm_dbowner=
# Si vous exécutez la version r11.2 ou ultérieure et souhaitez prendre en charge
# Oracle Bridging, définissez la valeur dsm_oracle_ddl sur 1
dsm_oracle_ddl=1
```

Activation d'une station d'accueil sous Windows

Les utilisateurs d'unité mobile doivent éventuellement échanger ou synchroniser les informations entre leur unité mobile et un ordinateur. En général, le périphérique mobile, par exemple un assistant numérique personnel (PDA), est relié via un "socle de synchronisation" ou une "unité d'ancrage" connecté au port série ou au port USB de l'ordinateur, ou directement à l'ordinateur via une interface infra-rouge ou Bluetooth.

Pour permettre l'échange de données entre le périphérique mobile et l'ordinateur à l'aide de l'unité d'ancrage, vous devez suivre les étapes d'installation et de configuration suivantes :

- Installez le logiciel de synchronisation.
    - Pour des unités Windows CE (PocketPC et Windows Mobile) :

      Installez Microsoft ActiveSync (livré avec le périphérique PocketPC ou Windows Mobile) sur un ordinateur cible, puis connectez l'unité à cet ordinateur.

      Remarque : Le composant Microsoft ActiveSync doit être installé avant l'activation de la prise en charge de station d'accueil sur un ordinateur PC hôte. En outre, le composant Microsoft ActiveSync doit être informé des modifications de la variable d'environnement PATH apportées au cours de l'installation de Client Automation. Pour cela, vous devez vous déconnecter, puis vous reconnecter après l'installation de Client Automation.
    - Pour les unités Palm OS :

      Installez le logiciel HotSync (Palm Desktop, livré avec l'unité Palm OS) sur un ordinateur cible, puis connectez l'unité Palm OS à cet ordinateur.
- Installez un agent Software Delivery ou Asset Management sur l'ordinateur cible.
- A partir du gestionnaire, activez l'unité proxy pour Client Automation, comme suit :
    - Créez une nouvelle stratégie de configuration, par exemple, ma_stratégie_stationdaccueil, puis définissez la valeur du paramètre DSM/common components/docking_devices avec la valeur True.
    - En outre, pour Software Delivery, attribuez la valeur Palm+WinCE au paramètre DSM/Agent/Common agent/software delivery docking device.
    - Appliquez la stratégie à l'ordinateur cible.
- Pour les périphériques Windows CE, reconnectez le périphérique à l'ordinateur cible (déconnectez puis reconnectez).

  Pour les périphériques Palm OS, synchronisez-les avec leur ordinateur hôte.
- Exécutez caf register all sur l'ordinateur hôte, ou patientez jusqu'à 24 heures pour un enregistrement automatique.

Exécution des agents à partir d'une source sous Windows

Client Automation autorise l'exécution sous Windows des composants des agents Asset Management, Software Delivery et Remote Control à partir d'un point d'installation de partage réseau administratif MSI. Cette fonction spécifique est appelée *exécution à partir de la source*. Si un agent a été installé en mode exécution à partir de la source, le programme exécutable est chargé et exécuté à partir de ce point d'installation de partage réseau administratif. Les fichiers de configuration, les fichiers journaux, etc. sont stockés sur le disque local.

Les composants communs CAM et CAWIN doivent toujours être installés localement.

Après l'installation d'un agent en mode exécution à partir de la source, le système de l'agent doit être redémarré.

Pour configurer un environnement en vue de l'installation d'agents en mode exécution à partir de la source, procédez comme suit :

1. Créez un point d'installation administrative MSI.

   Utilisez l'assistant d'installation interactive pour accéder au dossier WindowsProductFiles_x86 et appeler le fichier setup.exe /a. Cette opération crée un point d'installation pour le produit complet et tous ses composants.

   Si vous souhaitez effectuer l'installation de l'agent en mode silencieux ou installer uniquement un composant de l'agent, accédez à l'un des dossiers de l'agent sous WindowsProductFiles_x86 et exécutez la commande suivante :
   `msiexec /a msipackagename /qn /v*l %temp%\ITRMAdminAgt.log"`

   Remarque : Si vous souhaitez utiliser la commande msiexec pour plusieurs packages d'agents, assurez-vous d'utiliser le même dossier racine pour tous les agents.

2. Créez un partage réseau pour le point d'installation administrative que vous venez de créer (sauf s'il existe déjà). Vous devez le configurer comme un partage de session Null.

3. Installez le package MSI à partir du point d'installation de partage réseau administratif.

   Sur l'ordinateur cible sur lequel vous souhaitez installer l'agent en mode exécution à partir de la source, vous pouvez exécuter la commande suivante :

   ```
   msiexec /i \\servernode\adminshare\msipackagename ADDSOURCE=ALL
   AGENT_SERVER=servername CAF_START_SERVICE=0 /qn /v*l %temp%\DSMSetupRFS.log
   ```

   Elle installe silencieusement l'agent.

Vous pouvez également configurer un environnement pour installer des agents en mode exécution à partir de la source en utilisant l'option Installation personnalisée de l'assistant d'installation. Lancez l'assistant d'installation en utilisant un chemin d'accès UNC, *noeud serveur**partage admin MSI*\setup.exe, suivez les boîtes de dialogue de l'installation personnalisée et configurez chaque agent que vous souhaitez exécuter à partir de la source.

Remarque : Si le partage du réseau d'administration est hébergé par un serveur Windows 2003, vous devez éventuellement ajouter le compte d'ordinateur de l'agent au groupes Administrateurs du serveur Windows 2003.

Exécution des services Client Automation sous des comptes d'utilisateur Windows

Pendant que le cadre d'applications (CAF) s'exécute sous le compte système local, il arrive qu'un service Client Automation tel que l'agent Software Delivery doive être exécuté sous un compte d'administrateur. CAF permet cela via les options de commande caf suivantes :

setcreds

La commande caf setcreds définit les informations d'identification pour un service Client Automation. Seuls les agents Asset Management et Software Delivery sont pris en charge. Vous pouvez utiliser cette commande directement sur la console dans un actif ou dans un travail logiciel envoyé à plusieurs ordinateurs. Attention cependant à l'incorporation de mots de passe en texte brut dans un travail.

savecreds, loadcreds

La commande caf savecreds vous permet de stocker un ensemble d'informations d'identification pour différents ordinateurs et services dans un fichier chiffré. Ce fichier peut être transmis à de nombreux ordinateurs et appliqué à l'aide de la commande caf loadcreds. Ce fichier vous permet de spécifier différents mots de passe d'administrateur pour plusieurs ordinateurs, puisque chaque entrée du fichier est spécifique à un ordinateur. La commande caf loadcreds applique uniquement ces entrées à l'ordinateur local sur lequel elle est exécutée.

Exécution des Services Client Automation en tant qu'Administrateur

Sous Windows, une fonction CAF vous permet d'exécuter un module d'extension ou un service Client Automation en utilisant des informations d'identification d'utilisateur spécifiques. Cependant, seuls les utilisateurs du groupe d'administrateurs sont pris en charge ; aucun autre type d'utilisateur ne fonctionnera.

Pour exécuter un module d'extension ou un service, par exemple le service sdagent

1. Ouvrez une fenêtre d'invite de commande.
2. Définissez les informations d'identification de sdagent avec la commande suivante :
   `caf setcreds sdagent user administrator password` *xxx*
3. Testez son fonctionnement en exécutant la commande suivante :
   `caf start sdagent`

   Le programme sdagent (sd_jexec.exe) s'affiche dans le gestionnaire des tâches en tant qu'administrateur.

Introduction de vos propres certificats X.509 dans l'image d'installation

CA Client Automation utilise des certificats X.509 pour distinguer l'authentification de ses processus clients de celle d'un service nécessitant une authentification. Par exemple, X.509 est utilisé lorsque le composant Software Delivery se connecte à son serveur de modularité parent.

Une installation CA Client Automation comporte un jeu de certificats standard par défaut signé par un certificat racine CA. Le certificat racine public est installé sur chaque nœud au sein de l'entreprise.

Nous recommandons vivement à chaque entreprise de créer et de déployer son propre certificat racine, ses propres certificats d'identité d'hôte standard (BHI) et ses propres certificats spécifiques à l'application.

Pour plus de détails sur la création de certificats spécifiques à l'utilisateur final, consultez les Fonctionnalités de sécurité CA Client Automation. (page 407)

Pour créer de nouveaux certificats à l'aide de l'outil cacertutil, vous devez installer au moins un composant (Explorateur, agent Asset Management, etc.). L'outil cacertutil se trouve dans le dossier bin, sous le répertoire d'installation DSM.

Après avoir créé vos propres certificats spécifiques, remplacez les certificats standard par défaut dans l'image d'installation par vos nouveaux certificats avant de lancer l'installation ou le déploiement de composants DSM.

Après avoir remplacé les certificats dans l'image d'installation, le déploiement ou l'installation peut démarrer comme d'habitude.

Certificats par défaut pour Windows

Les certificats par défaut pour Windows se trouvent dans les dossiers suivants : Chaque dossier comporte la structure d'arborescence suivante Program Files\CA\DSM\bin qui contient les certificats importants.

- AgentBHW
- AgentAM
- AgentRC
- AgentSD
- AllAgents
- Serveur
- Gestionnaire
- Explorateur

Certificats par défaut pour Linux et UNIX

Les certificats par défaut pour Linux et UNIX se trouvent dans des sous-répertoires appelés certificats, dans les répertoires de package suivants :

- agent
- am_agent
- basichwinv
- rc_agent (Linux uniquement)
- sd_agent
- serveur (Linux uniquement)

Personnalisation de certificats X.509 à l'aide de cfcert.ini

Le fichier cfcert.ini contrôle les certificats installés par Client Automation. Le fichier cfcert.ini contient plusieurs sections, qui correspondent à chaque groupe d'applications dans l'installation. Voici un exemple de fichier cfcert.ini par défaut :

```
[CAF]
files=itrm_dsm_r11_root.der,basic_id.p12

[Configuration]
files=ccsm.p12

[Gestionnaire]
files=itrm_dsm_r11_cmdir_eng.p12

[Enregistrement]
files=registration.p12

[USD.Agent]
files=itrm_dsm_r11_sd_catalog.p12

[USD.Manager]
files=itrm_dsm_r11_agent_mover.p12,itrm_dsm_r11_sd_catalog.p12
```

```
[Fichiers]
itrm_dsm_r11_root.der=cacertutil import -i:itrm_dsm_r11_root.der -it:x509v3
basic_id.p12=cacertutil import -i:basic_id.p12 -
ip:enc:uAa8VNL4DKZlUUtFk5INPnr2RCLGb4h0 -h -t:dsmcommon
ccsm.p12=cacertutil import -i:ccsm.p12 -t:csm -
ip:enc:IWhun2x3ys7y1FM8Byk2LMs56Rr8KmXQ
itrm_dsm_r11_cmdir_eng.p12=cacertutil import -i:itrm_dsm_r11_cmdir_eng.p12 -
ip:enc:gYuzGzNcIYzWjHA6w542pW68E8FobJhv -t:dsm_cmdir_eng
itrm_dsm_r11_sd_catalog.p12=cacertutil import -i:itrm_dsm_r11_sd_catalog.p12 -
ip:enc:wdyZd4DXpx6j5otwKY0jSaOOVLLi0txQruDVOslGOlNIMZw96c85Cw -t:dsmsdcat
itrm_dsm_r11_agent_mover.p12=cacertutil import -i:itrm_dsm_r11_agent_mover.p12 -
ip:enc:sytOQtZteLopAt1CX0jIJUJcpqBWrb7G7VegY7F7udogc1c5kLIylw -t:dsmagtmv
registration.p12=cacertutil import -i:registration.p12 -
ip:enc:z5jLhmvfkaAF4DLMDp3TWuC7nG8yh3dfvmN668thfrU -t:dsm_csvr_reg
babld.p12=cacertutil import -i:babld.p12 -ip:enc:TrdWglmuNCdeOAfj2j3vMwywVbGnlIvX
-t:babld_server
dsmpwchgent.p12=cacertutil import -i:dsmpwchgent.p12 -
ip:enc:QWF8vknD5aZsU1j5RLzgt1NQgF5DcXj4v1vS4ewDzOA -t:ent_access
dsmpwchgdom.p12=cacertutil import -i:dsmpwchgdom.p12 -
ip:enc:sqb9qO2SGjbYqzIvwM7HEbx0M6UJk8Dc82EvUoDeJmE -t:dom_access
dsmpwchgrep.p12=cacertutil import -i:dsmpwchgrep.p12 -
ip:enc:x901eho57IZ19zg6g97rQetHjA1461na7nhBmJl7mcc -t:rep_access
```

```
[Balises]
dsmcommon=x509cert://DSM r11/CN=Generic Host Identity,O=Computer Associates,C=US
csm=x509cert://dsm r11/CN=Configuration and State Management,O=Computer
Associates,C=US
dsm_cmdir_eng=x509cert://dsm r11/cn=dsm directory synchronisation,o=computer
associates,c=us
dsmsdcat=x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer
Associates,C=US
dsmagtmv=x509cert://dsm r11/CN=DSM r11 Agent Mover,O=Computer Associates,C=US
dsm_csvr_reg=x509cert://dsm r11/CN=DSM Common Server Registration,O=Computer
Associates,C=US
babld_server=x509cert://dsm r11/cn=babld server,o=computer associates,c=us
ent_access=x509cert://dsm r11/CN=Enterprise Access,O=Computer Associates,C=US
dom_access=x509cert://dsm r11/CN=Domain Access,O=Computer Associates,C=US
rep_access=x509cert://dsm r11/CN=Reporter Access,O=Computer Associates,C=US
```

Chaque section du fichier cfcert.ini déclare les certificats qui doivent être installés par le programme d'installation associé. Le programme d'installation lit l'entrée files= à partir de sa section associée dans cfcert.ini et installe chaque certificat répertorié en retour, à l'aide de la commande située dans la section [Fichiers] du fichier cfcert.ini.

Par exemple, le programme d'installation du cadre d'applications communes (CAF) détecte qu'il doit installer les certificats itrm_r11_dsm_root.der et basic_id.p12. Dans la section [Fichiers], le programme d'installation de CAF détecte les commandes cacertutil associées à ces certificats dans les deux premières lignes, puis il exécute ces commandes.

La section [Balises] vous permet de créer de nouveaux certificats qui n'utilisent pas les URI de certificat standard. Lors de l'installation d'un noeud du gestionnaire DSM, les composants d'installation lisent cette section et configurent les profils de sécurité pour les URI appelés. Les balises et les URI répertoriés précédemment sont les paramètres Client Automation par défaut et sont utilisés s'ils sont absents du fichier cfcert.ini.

Par convention, les noms de fichier répertoriés dans l'entrée files= du fichier cfcert.ini sont les mêmes que les noms de fichier de certificat sous-jacent. Cela permet une maintenance simplifiée du fichier d'initialisation cfcert.ini.

Pour remplacer les certificats par défaut par le vôtre, modifiez chaque section individuelle et la section [Fichiers] pour refléter les nouveaux noms et mots de passe du certificat.

Important : Assurez-vous que les nouveaux certificats sont importés à l'aide des noms de balise corrects. Les balises sont spécifiées par -t: -mp. Pour plus d'informations et une liste des certificats disponibles, reportez-vous aux sections Installation de certificats spécifiques à l'application (page 417) et Certificats actuels (page 583).

Modifier ou réparer une installation

Pour modifier ou réparer une installation de Client Automation existante, exécutez le programme d'installation. Les options disponibles sont les suivantes :

Modifier

Vous permet d'ajouter ou de supprimer des composants.

Remarque : N'oubliez pas de toujours indiquer l'état final du processus de modification. Si un gestionnaire est installé et que vous souhaitez ajouter un explorateur DSM, assurez-vous d'avoir coché Gestionnaire et Explorateur DSM, car il s'agit de l'état final souhaité.

Réparer

Vous permet de réparer une installation existante. La fonction Réparer vérifie les fichiers, les clés de registre et les raccourcis de l'installation originale et les réinstalle s'ils ont été supprimés ou corrompus.

Modification d'une installation

La modification d'une installation existante de Client Automation signifie installer de nouvelles fonctionnalités ou supprimer des fonctionnalités actuellement installées.

Pour modifier une installation

1. Exécutez le programme d'installation, puis sélectionnez l'option Installer Client Automation.

   Le programme d'installation détecte si une installation existe déjà et affiche la boîte de dialogue Sélectionner l'option d'installation.

2. Sélectionnez Modifier.

   La boîte de dialogue Sélectionner une fonctionnalité de produit s'affiche.

3. Faites vos choix, puis cliquez sur Suivant.

   La boîte de dialogue Sélectionner les fonctions qui s'affiche propose toutes les fonctions disponibles. Les fonctions installées sont déjà sélectionnées.

4. Sélectionnez les fonctions à installer et désélectionnez les fonctions à supprimer.
5. Suivez les instructions de l'assistant d'installation.

Une fois l'opération terminée, vous pouvez redémarrer immédiatement le service CAF ou indiquer de redémarrer le service ultérieurement.

Modification le rôle de gestionnaire

Le changement du rôle d'un gestionnaire DSM de gestionnaire de domaine à gestionnaire d'entreprise ou de gestionnaire d'entreprise à gestionnaire de domaine ne peut être effectué par le biais de la fonction Modifier. Pour passer d'un rôle de gestionnaire à l'autre, procédez comme suit :

- Utilisez la fonction Modifier pour désinstaller le gestionnaire.
- Désinstallez le fournisseur de base de données et la base de données de gestion (MDB).

  Important : Avant de désinstaller le fournisseur de base de données, consultez la section Désinstallation du gestionnaire et de la base de données de gestion. (page 225)

- Utilisez la fonction Modifier pour installer le gestionnaire avec son nouveau rôle.

Réparation d'une installation

La réparation d'une installation existante de Client Automation répare les fichiers, raccourcis et entrées de registre manquants ou corrompus de l'installation précédente.

Pour réparer une installation :

1. Exécutez le programme d'installation, puis sélectionnez l'option Installer Client Automation.

   Le programme d'installation détecte si une installation existe déjà et affiche la boîte de dialogue Sélectionner l'option d'installation.

2. Sélectionnez Réparer.
3. Suivez les instructions de l'assistant d'installation.

La fonction Réparer ne remplace pas les fichiers ou les paramètres créés ou réalisés au cours de l'utilisation de Client Automation.

Mise à niveau d'une installation

La mise à niveau d'une installation signifie réinstaller des fonctions ou des composants de versions ultérieures, sans désinstaller les précédents. Tous les paramètres en cours sont conservés et la base de données n'est pas remplacée.

Vous pouvez effectuer une mise à niveau à l'aide de l'une des méthodes suivantes :

En utilisant l'assistant d'installation

Exécutez le programme d'installation, qui vous informe qu'une version antérieure a été détectée et qu'une mise à niveau sera effectuée.

En utilisant l'explorateur DSM et en distribuant les packages pour la mise à niveau

Au sein de l'explorateur DSM, les packages Software Delivery pré-enregistrés peuvent être utilisés pour distribuer les composants. Software Delivery exécute automatiquement une mise à niveau si une version antérieure existe sur l'ordinateur cible.

En utilisant l'assistant de déploiement

Au sein de l'explorateur DSM, l'assistant Déploiement de l'infrastructure peut être utilisé pour distribuer et installer des packages sur les ordinateurs cibles. Pour les ordinateurs cibles sur lesquels une version antérieure est déjà installée, vous devez effectuer une mise à niveau à partir de la page de l'assistant Déploiement : Configuration de l'agent. Dans le champ d'entrée Options d'installation Windows supplémentaires, les paramètres suivants doivent être saisis pour exiger une mise à niveau sur l'ordinateur cible :

```
REINSTALL=ALL REINSTALLMODE=vomus
```

Appel direct des packages MSI

Lorsque vous utilisez directement les packages MSI, vous devez ajouter les paramètres suivants à la ligne de commande :

```
REINSTALL=ALL, REINSTALLMODE=vomus
```

Exemple

```
msiexec.exe /i"N:\DSM_12_0_1234_1_DVD\WindowsProductFiles_x86\AgentSD\agtsd.msi"

REINSTALL=ALL
REINSTALLMODE=vomus /l*v "%temp%\ITRMupdateSDagent.log"
```

Désinstallation de Client Automation

Les méthodes pour désinstaller Client Automation ou des parties de l'installation Client Automation sont proposées dans les sections suivantes :

- Désinstallation de Client Automation sous Windows (page 242)
- Désinstallation de Client Automation sous Linux et UNIX (page 244)

Désinstallation de Client Automation sous Windows

Pour désinstaller Client Automation totalement ou partiellement, vous pouvez utiliser l'*une* des options suivantes :

- Utiliser la fonction Ajout/Suppression de programmes à partir du Panneau de configuration Windows.

  Cette fonction vous permet de supprimer l'intégralité ou des composants uniques de Client Automation. Sélectionnez l'élément approprié dans la liste des logiciels installés et cliquez sur le bouton Modifier/Supprimer.

- Utilisez l'assistant d'installation Client Automation.

  Exécutez setup.exe. L'assistant d'installation démarre et vous guide tout au long de la désinstallation interactive. Choisissez Installer Client Automation. L'une des boîtes de dialogue suivantes vous propose les options Supprimer, Modifier et Réparer.

  L'option Supprimer permet de supprimer l'intégralité de l'installation Client Automation du système où setup.exe a été exécuté.

  L'option Modifier permet d'obtenir une liste de tous les composants et fonctions gérés par le programme d'installation. Les fonctions actuellement installées sur le système local sont cochées. Effacez les coches (le crochet disparaît) correspondant aux composants ou fonctions que vous souhaitez désinstaller. Lorsque vous fermez la boîte de dialogue, les fonctions spécifiées sont désinstallées, mais l'installation de Client Automation n'est pas supprimée.

- Exécutez msiexec /x avec un code de produit approprié dans la ligne de commande.

  Le composant à supprimer est spécifié par son code de produit (page 243). L'utilisation de l'option /qn dans la commande msiexec vous permet de spécifier une désinstallation en mode silencieux.

Sous Windows, la désinstallation à l'aide du programme d'installationdésinstalle tous les produits et les packs linguistiques Client Automation. La désinstallation de packages MSI individuels à l'aide de l'option Ajouter/Supprimer des programmes du panneau de configuration Windows ou de l'outil de ligne de commande msiexec ne désinstalle aucun autre package MSI.

Remarque : Après la désinstallation sous Windows, certains fichiers, dossiers et clés de registre demeurent. Une fois la désinstallation terminée, supprimez manuellement le répertoire DSM.

Codes de produit dans Client Automation

Les composants de Client Automation pouvant être installés sont identifiés à l'aide d'un code de produit individuel, comme suit :

Agent d'inventaire de base (ENU et multilingue) :

{501C99B9–1644–4FC2–833B–E675572F8929}

Agent Asset Management (ENU et multilingue) :

{624FA386-3A39-4EBF-9CB9-C2B484D78B29}

Agent de service de transport de données (ENU et multilingue) :

{C0C44BF2–E5E0–4C02–B9D3–33C691F060EA}

Agent Remote Control (ENU et multilingue) :

{84288555–A79E–4ABD–BA53–219C4D2CA20B}

Agent Software Delivery (ENU et multilingue) :

{62ADA55C–1B98–431F–8618–CDF3CE4CFEEC}

Package linguistique DEU de l'agent :

{6B511A0E-4D3C-4128-91BE-77740420FD36}

Package linguistique FRA de l'agent :

{9DA41BF7-B1B1-46FD-9525-DEDCCACFE816}

Package linguistique JPN de l'agent :

{A4DA5EED-B13B-4A5E-A8A1-748DE46A2607}

Package linguistique ESN de l'agent :

{94163038-B65E-45BE-A70C-DC319C43CFF2}

Package linguistique KOR de l'agent :

{2C300042-2857-4E6B-BC05-920CA9953D2C}

Package linguistique CHS de l'agent :

{2D3B15F5-BBA3-4D9E-B7AB-DC2A8BD6EAD8}

Documentation :

{A56A74D1–E994–4447–A2C7–678C62457FA5}

Explorateur :

{42C0EC64–A6E7–4FBD–A5B6–1A6AD94A2D87}

Gestionnaire :

{E981CCC3–7C44–4D04–BD38–C7A501469B37}

Installation principale :

{C163EC47–55B6–4B06–9D03–2A720548BE86}

Serveur de modularité :

{9654079C-BA1E-4628-8403-C7272FF1BD3E}

DMPrimer :

{A312C331-2E7A-42E1-9F31-902920C402EE}

Exemple de désinstallation à l'aide de msiexec et du code de produit

L'exemple suivant supprime l'agent Asset Management en mode silencieux et écrit les informations de suppression dans un fichier journal, rmvamagt.log, dans le dossier de journalisation sur le lecteur C.

```
msiexec /x {A302890B-3180-455B-A958-6DDFAE9F4B00} /l*v "c:\logs\rmvamagt.log" /qn
```

Désinstallation de Client Automation sous Linux et UNIX

Vous pouvez désinstaller totalement ou partiellement Client Automation sous Linux ou UNIX en utilisant l'une des options suivantes :

./setup.sh

Exécutez setup.sh à partir du DVD d'installation puis sélectionnez Désinstaller dans la boîte de dialogue d'installation.

lsm -e *prodname* [-s]

Exécutez cette version de la commande lsm à partir de la ligne de commande Client Automation. Dans la commande lsm, le produit ou le composant est spécifié par le paramètre *prodname*. L'option -s indique le mode de désinstallation autonome (silencieux).

L'exemple suivant désinstalle l'intégralité de Client Automation en mode autonome (silencieux) :

```
lsm -e ca-dsm -s
```

L'exemple suivant désinstalle le composant DMPrimer :

```
lsm -e ca-dsm-dmprimer-standalone
```

Les noms de produit ou de composant pouvant être utilisés comme valeurs pour la variable *prodname* dans la commande du programme d'installation (lsm) Linux/UNIX sont répertoriés dans le tableau ci-dessous :

Nom du produit/composant	Description
ca-dsm	CA Client Automation
ca-dsm-dmprimer-standalone	DMPrimer (installé uniquement à l'aide du composant de déploiement d'infrastructure de Client Automation)
ca-dsm-SMPackager	Outil de packaging de logiciels pour Linux et UNIX

Remarques générales sur la désinstallation de l'agent

La désinstallation du package de base d'un agent désinstalle également tous les packages linguistiques associés.

La désinstallation d'un package linguistique n'affecte pas le package de base de l'agent, c'est pourquoi vous pouvez supprimer les packages linguistiques à tout moment.

Quand un package linguistique autonome est désinstallé et que la langue actuelle dans le magasin de configurations est définie sur cette langue, la valeur du paramètre de configuration, itrm/common/localization/language, dans le magasin de configurations devient enu. Dans le cas contraire, la valeur du paramètre ne change pas.

Les packages linguistiques annulent leur enregistrement auprès des fonctionnalités Software Delivery et Déploiement de l'infrastructure lors de leur désinstallation.

Désinstallation des packages DSM de l'agent pour Windows à l'aide de Software Delivery

Les packages DSM peuvent être divisés en deux classes : les packages de base et les packages personnalisés. Les packages personnalisés contiennent les packages de base, qui représentent les "atomes." Les packages de base sont enregistrés dès leur installation ou détection, et sont répertoriés comme des logiciels installés. Lors de la livraison et de l'installation d'un package au moyen de Software Delivery, un enregistrement d'installation est créé pour le package personnalisé. Néanmoins, cet enregistrement d'installation du package personnalisé n'est pas créé en cas d'installation manuelle ou d'installation via le déploiement d'infrastructure.

Lors de la désinstallation des packages DSM via Software Delivery, seuls les packages de base doivent être désinstallés. L'ordre de désinstallation des packages de base est important. Désinstallez tout d'abord les packages de langues de l'agent, puis le module d'extension DCS, et enfin le collecteur d'actifs et/ou Remote Control. L'agent Software Delivery doit bien sûr être désinstallé en dernier. Vous pouvez créer, par exemple, un conteneur de job de livraison de logiciel comprenant un job pour chaque étape. Une fois les packages de base désinstallés, supprimez les enregistrements d'installation des packages personnalisés à l'aide de l'explorateur DSM.

Remarque : Les modules d'extension tels que l'adaptateur de socket sécurisé et DMPrimer ne sont pas supprimés. Pour supprimer ces modules d'extension, désinstallez manuellement tous les composants DSM non désinstallés sur l'ordinateur cible au moyen de l'option Ajout/Suppression de programmes.

Chapitre 5: Déploiement de l'infrastructure

La présentation suivante concerne les phases du déploiement d'infrastructure, les concepts de gestion du déploiement et les méthodes de déploiement interactives, par le biais de la ligne de commande, ou déclenchées par la découverte continue. En outre, certains aspects, conditions préalables et outils spéciaux du déploiement sont étudiés.

Ce chapitre traite des sujets suivants :

Introduction au déploiement de l'infrastructure

Deployment Management (DM) est la solution de déploiement de l'infrastructure commune au sein de CA Client Automation. DM simplifie le déploiement de l'infrastructure de composants logiciels sur un grand nombre d'ordinateurs cibles au sein d'une entreprise hétérogène, sans nécessiter la connexion manuelle d'un administrateur, le transfert des images d'installation, l'exécution du processus d'installation et la surveillance des résultats de l'installation sur chaque ordinateur à tour de rôle.

DM offre les avantages suivants :

- Déploiement automatique de l'infrastructure sur une large gamme d'environnements d'exploitation cibles.
- Déploiement synchrone, c'est-à-dire qu'un déploiement initialisé se conclut par l'installation du composant déployé et son exécution sans autre intervention humaine. Lorsque cela n'est pas possible, le déploiement asynchrone est proposé ; il peut impliquer qu'un utilisateur se connecte ou redémarre avant la fin de l'installation.
- Fonctions améliorées de journalisation et de création de rapports. DM surveille la progression d'un déploiement et affiche des informations appropriées sur l'état.
- Fonctionnalités de sécurité correspondant aux besoins des installations actuelles des entreprises. Des technologies de chiffrement et d'authentification adaptées sont utilisées pour garantir qu'aucune donnée sensible n'est accessible par des tiers lors de la transmission réseau ou du stockage permanent.
- Un gestionnaire de déploiement séparant l'essentiel de la charge de travail de déploiement des interfaces client de déploiement. Plusieurs gestionnaires de déploiement peuvent se déployer sur un seul ordinateur cible, si nécessaire.
- Déploiement automatique vers des systèmes nouvellement découverts. L'administrateur peut définir des règles afin de déployer des logiciels spécifiques sur certains systèmes, dès qu'un ordinateur apparaît pour la première fois sur le réseau.

Phases de déploiement d'infrastructure Client Automation typiques

Le déploiement de l'infrastructure se compose des principales phases suivantes :

- Installation interactive du gestionnaire au siège
- Définition des serveurs de modularité pour ce gestionnaire et déploiement des serveurs de modularité, à l'aide de l'assistant de déploiement.
- Déploiement des agents connectés aux serveurs de modularité, à l'aide de l'assistant de déploiement.
- Déploiement automatique vers des systèmes nouvellement détectés.

Concepts de gestion du déploiement

Lorsqu'une opération de déploiement est requise, le gestionnaire tente d'abord d'envoyer un package de logiciel d'injection relativement petit vers l'ordinateur cible.

Le package du logiciel d'injection est écarté en utilisant l'une des nombreuses méthodes existantes, en fonction du système d'exploitation cible et des logiciels installés.

Il n'est pas toujours possible d'écarter à distance le logiciel d'injection, notamment lorsque les paramètres de sécurité du réseau l'interdisent. Néanmoins, il est possible dans de tels cas d'installer manuellement le logiciel d'injection sur des ordinateurs cibles.

Une fois le logiciel d'injection installé, il est utilisé pour transférer les données du package de déploiement actuel vers l'ordinateur cible et exécuter l'installation. Tous les déploiements ultérieurs vers le même ordinateur cible peuvent utiliser l'installation existante du logiciel d'injection.

Le gestionnaire de déploiement contrôle toutes les opérations de déploiement et gère l'état des jobs.

Les clients du déploiement (interface de l'assistant de déploiement et de la ligne de commande dmsweep) utilisent une API pour communiquer avec le gestionnaire du déploiement. Ils sont installés avec l'explorateur DSM et peuvent par conséquent être exécutés sur un ordinateur autre que le gestionnaire, si nécessaire.

Pour réduire l'utilisation du réseau lors du déploiement d'un grand nombre d'agents, vous pouvez transférer les packages de déploiement vers les serveurs de modularité.

Protocoles de transfert de packages à l'aide du serveur de modularité

DMDeploy utilise les protocoles suivants pour transférer des packages vers des ordinateurs cibles lors du déploiement via un serveur de modularité :

Partage réseau Windows

Utilisez ce mécanisme lorsque le serveur de modularité et l'ordinateur cible fonctionnent sous Windows.

SSH/SFTP

Utilisez ce mécanisme lorsque le serveur de modularité ou l'ordinateur cible fonctionne sous Linux ou UNIX.

Telnet/FTP

Utilisez ce mécanisme lorsque le serveur de modularité ou l'ordinateur cible fonctionne sous Linux ou UNIX.

Pour plus d'informations sur ces mécanismes de transfert, consultez la section Conditions préalables pour le déploiement automatique de l'infrastructure Client Automation (page 268).

Utilisation de serveurs de modularité dans le contexte d'un déploiement d'infrastructure

Pour réduire l'utilisation du réseau lors du déploiement d'un grand nombre d'agents, vous pouvez transférer les packages de déploiement vers les serveurs de modularité. Pour que les packages de charge utile du déploiement soient accessibles sur un serveur de modularité, déployez la charge utile vers le serveur de modularité, mais activez l'option Transfert de packages sur le serveur de modularité. Pour déployer par la suite les packages stockés sur le serveur de modularité, cochez l'option Transférer les packages à partir du serveur de modularité lorsque vous sélectionnez la charge utile du déploiement.

L'utilisation d'un serveur de modularité avec le déploiement de l'infrastructure affecte la configuration du réseau. En général, un serveur de modularité doit être utilisé pour déployer des agents vers des ordinateurs cibles "proches" sur le réseau d'entreprise, c'est-à-dire ceux qui utilisent un débit de réseau relativement élevé entre le serveur de modularité et les ordinateurs agents.

Les tâches d'administration à effectuer sont nombreuses et n'oubliez pas d'inclure les éléments suivants lors de l'utilisation de serveurs de modularité avec le déploiement de l'infrastructure.

- Pour déployer vers des ordinateurs cibles Windows à l'aide d'un serveur de modularité Linux avec le mécanisme de transfert Telnet/FTP, vous devez activer Telnet sur les ordinateurs cibles Windows. Sur les ordinateurs exécutant Windows 2003, Windows XP ou des systèmes d'exploitation plus récents, vous devez activer et démarrer le service Telnet dans la boîte de dialogue Outils d'administration, Services, accessible à partir du Panneau de configuration Windows.

- Pour un déploiement vers des ordinateurs cibles Linux ou UNIX à l'aide d'un serveur de modularité, vous devez activer un serveur FTP doté du mécanisme Telnet/FTP sur le serveur de modularité. En outre, l'ordinateur cible requiert un serveur Telnet en cours d'exécution car le gestionnaire utilise Telnet pour transférer le package sur l'ordinateur cible et FTP pour le transférer sur le serveur de modularité.

  D'autre part, si le serveur de modularité fonctionne sur un ordinateur Windows, vous devrez effectuer l'opération de configuration suivante sur celui-ci pour désigner un autre site FTP à utiliser par Déploiement d'infrastructure. Vous devez désigner un autre site FTP pour éviter les problèmes de sécurité avec d'autres zones FTP lors du partage du dossier de transfert où seront stockés les agents Client Automation :

  - Ouvrez le Panneau de configuration, cliquez sur Outils d'administration et sélectionnez le Gestionnaire des services Internet (IIS).
  - Cliquez avec le bouton droit sur le noeud Sites FTP et sélectionnez Nouveau, Site FTP pour lancer l'Assistant Création de site FTP.
  - Lancez l'Assistant et entrez Site FTP ITCM comme description du nouveau site. Sélectionnez les options par défaut proposées par l'assistant jusqu'à la page Répertoire de base du site FTP. A cette page, spécifiez le dossier d'installation de DMPrimer, cet emplacement étant celui où les agents Déploiement d'infrastructure ITCM seront transférés. Si un DMPrimer est déjà installé, cliquez sur Parcourir pour accéder à son dossier. Par défaut, le DMPrimer est installé dans Program Files\CA\DSM\DMPrimer. Une fois le dossier du site FTP sélectionné, poursuivez dans l'assistant en sélectionnant les options par défaut, puis cliquez sur le bouton Terminer.

  Remarque : Lorsque vous utilisez le serveur de modularité de Windows pour effectuer un déploiement sur des ordinateurs Linux, le site FTP Client Automation doit fonctionner. Assurez-vous que les autres sites FTP tels que le site FTP par défaut sont arrêtés. Sinon, le déploiement échouera.

- Lors de l'utilisation de FTP sur un serveur de modularité, vous devez être attentif lors de la spécification des informations d'identification d'utilisateur requises pour s'y connecter. Pendant le transfert d'un package vers le serveur de modularité/FTP, vous devez spécifier les informations d'identification d'un utilisateur disposant d'un privilège d'écriture sur le serveur de modularité. Lors du déploiement d'un package à partir d'un serveur de modularité/FTP, l'utilisateur anonyme est généralement habitué à accéder aux packages.

- Si un déploiement via Telnet/FTP est nécessaire, les détails du serveur FTP sont fournis pendant l'installation du gestionnaire et les packages DMPrimer sont téléchargés vers le serveur spécifié. En règle générale, le serveur FTP se trouve sur le même ordinateur qu'un serveur de modularité.

  Si plusieurs serveurs FTP sont utilisés avec un seul gestionnaire de déploiement de l'infrastructure, par exemple si plusieurs serveurs de modularité s'exécutent sur chaque ordinateur avec un serveur FTP, vous devez effectuer quelques opérations de configuration manuelle avant que le déploiement utilise un autre serveur FTP non configuré au moment de l'installation.

  Pour modifier les informations FTP, vous devez exécuter la commande "dmdeploy ftpinfo" avec les informations du nouveau serveur FTP et copier les packages du logiciel d'injection et le fichier dmkeydat.cer à l'emplacement correspondant sur le serveur FTP. Le gestionnaire de déploiement utilise alors ce serveur FTP pour effectuer un déploiement via Telnet/FTP. Ces étapes sont traitées dans la section Modification des détails de serveur FTP pour une utilisation avec le déploiement de l'infrastructure. (page 271)

- Si vous utilisez un serveur de modularité sur Windows pour le déploiement d'infrastructure, notez que Windows limite le nombre de connexions simultanées. Certains jobs peuvent échouer lorsque la limite de connexions est atteinte. Dans ce cas, vous recevez le message *Impossible d'obtenir le package actuellement. Limite de connexions atteinte sur le serveur de modularité. Réessayez.* Utilisez le paramètre de configuration Limite du thread de déploiement afin de contrôler le nombre de déploiements simultanés exécutés par le gestionnaire de déploiement de l'infrastructure. La valeur par défaut du paramètre de configuration est 10 et peut être modifiée si vous effectuez un déploiement via un serveur de modularité exécuté sous Windows.

- Dans un environnement purement IPv6, le déploiement échoue si les versions de Telnet utilisées ne prennent pas en charge le protocole IPv6.

- Dans un environnement purement IPv6, le déploiement sur des ordinateurs cibles Linux ou UNIX échoue si les versions de FTP utilisées ne prennent pas en charge le protocole IPv6.

Informations complémentaires :

Protocoles de transfert de packages à l'aide du serveur de modularité (page 250)

Audit de serveurs de modularité avec un contenu de déploiement d'infrastructure

Le déploiement de l'infrastructure permet aux utilisateurs d'auditer les serveurs de modularité dans leur réseau qui contiennent un contenu de déploiement. Il leur permet en outre d'obtenir une liste de packages de déploiement qui existent sur chaque serveur de modularité.

La liste de packages de déploiement d'infrastructure disponibles sur un serveur de modularité s'affiche lorsque le serveur de modularité est sélectionné, au cours de la navigation via l'assistant de déploiement. Le contenu du serveur de modularité peut également être affiché à l'aide de la commande dmsweep sspack.

Processus de gestion du déploiement

Lors de l'exécution de Deployment Management (DM), les principales étapes du processus de déploiement sont les suivantes :

1. Depuis l'ordinateur de l'administrateur, le composant client de déploiement d'infrastructure (assistant de déploiement ou commande dmsweep) émet une demande vers le gestionnaire DM (DMDeploy), afin d'installer un agent sur une liste composée d'un ou de plusieurs ordinateurs cibles. Le gestionnaire de déploiement peut être exécuté sur un ordinateur distant du client. La liste des cibles peut être constituée de noms d'ordinateur explicites ou d'adresses IPv4. Vous pouvez également l'obtenir à partir d'une source de "conteneur", telle qu'un domaine Windows, un répertoire LDAP ou une requête Client Automation.

   Afin que le déploiement réussisse sur chaque ordinateur cible, il est important de vérifier que son nom, qu'il soit entré explicitement ou obtenu auprès d'un conteneur, corresponde à la résolution d'adresse de la cible, comme affichée sur l'ordinateur du gestionnaire de déploiement. Si, par exemple, la liste des cibles extraite d'un répertoire n'est pas complète avec des noms de domaine réseau, le déploiement risque de ne pas pouvoir continuer dans certaines configurations réseau.

2. Une vérification est effectuée pour voir si DMPrimer est déjà installé sur l'ordinateur cible. Si ce n'est pas le cas, DMPrimer est d'abord installé sur l'ordinateur cible. Le gestionnaire DM tente de livrer le package d'installation DMPrimer. La méthode de distribution utilisée dépend de l'environnement d'exploitation cible et de la sécurité activée dans cet environnement. Une fois l'image DMPrimer copiée à travers l'ordinateur cible, son installation est initiée.

   Certains systèmes d'exploitation ne disposant pas de méthode d'invocation distante de l'installation de DMPrimer, il est parfois nécessaire d'établir le programme d'installation à installer sur un événement significatif de système d'exploitation, comme un redémarrage. Il s'agit d'une installation asynchrone, car le message indiquant la fin de l'installation est reçu de façon asynchrone, à un moment non spécifié. L'installation de DMPrimer peut aussi être effectuée manuellement.

3. Le programme d'installation DMPrimer s'installe et installe également le composant de CA Message Queuing (CAM) sur l'ordinateur cible. Pendant l'installation, le mode FIPS de DMPrimer sur l'ordinateur cible est fonction du mode FIPS du gestionnaire. Le gestionnaire transfère le mode FIPS comme s'il s'agissait d'un paramètre d'installation. Ce paramètre est également actualisé dans le fichier dmprimer.cfg, qui est partie de l'installation de DMprimer.

   Toutefois, à chaque démarrage, le logiciel DMPrimer lit d'abord le mode FIPS dans la stratégie de configuration de l'agent sur l'ordinateur cible. S'il y parvient, le logiciel d'injection actualise le fichier dmprimer.cfg avec le mode FIPS de l'agent et démarre dans ce mode. Si aucun agent n'est installé sur la cible, DMPrimer démarre dans le mode indiqué dans le fichier dmprimer.cfg.

   Remarque : Sous la plupart des systèmes d'exploitation, l'installation de DMPrimer doit être exécutée avec des privilèges élevés.

4. Une fois que DMPrimer est installé et que DMDeploy a reçu le signal de "fin d'installation" provenant de l'ordinateur cible, le déploiement du package peut commencer. Un gestionnaire DMDeploy ayant préalablement installé un DMPrimer et s'étant authentifié auprès de celui-ci peut déployer des packages sans devoir fournir à nouveau des noms d'utilisateur ou des mots de passe. Il y parvient grâce à une authentification, en utilisant des clés publiques et privées. Vous pouvez forcer un gestionnaire de déploiement à retransférer et à installer DMPrimer, même si une version est déjà présente. Pour cela, définissez la stratégie de configuration "AlwaysDeployPrimer" à l'aide de l'explorateur DSM.

Pour plus de détails sur l'utilisation du gestionnaire de déploiement via l'explorateur DSM, consultez l'Aide en ligne de l'assistant de déploiement.

Spécification flexible de cibles de déploiement

Pour garantir une certaine souplesse lors de la spécification des cibles de déploiement, un fichier d'informations d'identification cible a été introduit. Avec ce fichier, un administrateur peut créer et gérer des listes de systèmes cibles individuels ou des groupes de systèmes cibles avec leurs informations d'identification de connexion.

Le fichier d'informations d'identification cible permet aux utilisateurs de planifier leur déploiement hors-ligne, avant d'initier les travaux de déploiement réels. Vous pouvez spécifier un déploiement vers d'autres zones d'un réseau en créant des familles de fichiers d'informations d'identification comme, par exemple, des fichiers propres à d'autres services de l'entreprise.

Vous pouvez utiliser le fichier d'informations d'identification cible avec la commande dmsweep (à l'aide de l'option /targetcred) et l'assistant Déploiement de l'infrastructure.

Transfert d'options vers l'installation DMPrimer

Vous pouvez spécifier des options pour l'installation DMPrimer. Cela vous permet, par exemple, d'installer DMPrimer à des emplacements qui ne sont pas standard. Il s'agit d'une condition requise courante, car touts les installations suivantes de composants Client Automation sur un ordinateur spécifique doivent utiliser les paramètres d'emplacement préalablement définis lors de l'installation de DMPrimer. Par conséquent, si vous devez utiliser des emplacements d'installation différents de ceux par défaut pour le logiciel Client Automation, vous devez définir l'emplacement d'installation de DMPrimer à l'aide des options décrites ci-dessous lors du déploiement initial vers un ordinateur cible spécifique.

Vous pouvez entrer les options d'installation via la ligne de commande dmsweep (à l'aide de l'option /primerargs) et de l'assistant de déploiement (à l'aide de la zone Afficher des options avancées de la page Configuration d'agent).

Pour installer DMPrimer à un emplacement non standard, vous devez transférer les arguments suivants vers l'installation DMPrimer :

- Pour un déploiement vers des ordinateurs cibles Windows :

  `CA=x:\`*`CheminNouveauProduit`*

  `CASHCOMP=x:\`*`NouvelleZonePartagée`*

Pour un déploiement vers des ordinateurs cibles Linux ou UNIX :

```
/RCA_ITRM_BASEDIR=/opt/CheminNouveauProduit
/RCASHCOMP=/opt/NouvelleZonePartagée
```

Par défaut, les installations de DMPrimer utilisent le même mode FIPS que le gestionnaire. Vous pouvez remplacer la valeur par défaut au moyen du paramètre suivant :

Ordinateurs cibles Windows :

```
FIPS_MODE=1 //(FIPS-preferred)
FIPS_MODE=2 //(FIPS-only)
```

Ordinateurs cibles Linux ou UNIX :

```
/RITCM_FIPS_MODE=1 //(FIPS-preferred)
/RITCM_FIPS_MODE=2 //(FIPS-only)
```

Remarque sur l'ajout d'options d'installation Windows

Lorsque vous transmettez des options d'installation Windows supplémentaires, contenant un ou plusieurs espaces vers un job de déploiement, en utilisant pour cela la page de configuration de l'agent de l'assistant de déploiement de l'infrastructure, vous devez insérer correctement les guillemets dans les paramètres. Pour chaque option d'installation de Windows supplémentaire, la valeur doit être mise entre guillemets ("), par exemple :

```
CA="C:\Program Files\mydir" CASHCOMP="C:\Program Files\mydir\sharedComps"
```

Sur la ligne de commande, lors de l'utilisation de dmsweep, les paramètres individuels doivent être séparés par des virgules et protégés par des guillemets, comme dans l'exemple suivant :

```
/pri "CA=\"C:\Program Files\CA\test\" CASHCOMP=\"C:\Program Files\CA\test\""
```

Remarques sur le déploiement de l'infrastructure à l'aide d'adresses IPv6

Si vous êtes sur le point de déployer l'infrastructure CA Client Automation à l'aide d'IPv6, vous devez lire attentivement les remarques suivantes :

- Afin de pouvoir utiliser le Déploiement de l'infrastructure dans un environnement IPv6, les conditions suivantes doivent être remplies :

  1. La clé de registre suivante doit être définie sur 1 dans le gestionnaire DSM :

     HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)

  2. Appliquez deux mises à jour de correctif sur le serveur de modularité :

     - http://support.microsoft.com/kb/947369/en-us
     - http://support.microsoft.com/kb/950092/en-us

  3. Le nom d'hôte de l'ordinateur cible doit correspondre à une adresse IPv6 globale.

     Assurez-vous également que la recherche inversée de l'adresse IPv6 renvoie le même nom d'hôte.

  4. L'option Utiliser des noms d'hôtes de la stratégie de configuration Déploiement de l'infrastructure, doit être définie sur True.

  Remarque : Si vous avez l'intention d'utiliser Déploiement d'infrastructure pour déployer des logiciels par l'intermédiaire d'un serveur de modularité sur un ordinateur Windows 2003 en environnement IPv6, vous devrez aussi exécuter les étapes 1 à 3 ci-dessus sur l'ordinateur cible Windows 2003.

  Si ces conditions ne sont pas remplies dans un réseau IPv6 pur, le package DMPrimer doit être installé manuellement. Pour plus d"informations, consultez la section Installation manuelle du logiciel d'injection de déploiement de l'infrastructure. (page 257)

- Les fonctionnalités Déploiement de l'infrastructure et Détection continue prennent en charge le déploiement uniquement vers les plages d'adresses IPv4.

Installation manuelle du logiciel d'injection de déploiement de l'infrastructure

Même si le déploiement automatique n'est pas possible vers les ordinateurs cibles pour une raison ou une autre, le déploiement du logiciel d'infrastructure reste possible si vous installez manuellement le logiciel d'injection sur l'ordinateur cible. Cela peut être effectué grâce à l'installation physique du package du logiciel d'injection ou à l'exécution de l'installation via des scripts de connexion.

Outre l'installation du logiciel d'injection, vous devez installer une clé de sécurité générée par le gestionnaire de déploiement que vous souhaitez utiliser pour déployer l'infrastructure vers les ordinateurs cibles.

Le programme d'installation du logiciel DMprimer offre la possibilité d'activer le mode FIPS au niveau du logiciel d'injection. Si vous souhaitez modifier le mode FIPS après l'installation, actualisez le paramètre FIPS_MODE dans le fichier dmprimer.cfg. Toutefois, à chaque démarrage, le logiciel DMPrimer lit d'abord le mode FIPS dans la stratégie de configuration de l'agent sur l'ordinateur cible. S'il y parvient, le logiciel d'injection actualise le fichier dmprimer.cfg avec le mode FIPS de l'agent et démarre dans ce mode. Si aucun agent n'est installé sur la cible, DMPrimer démarre dans le mode indiqué dans le fichier dmprimer.cfg.

Installation de Deployment Primer sous Windows

L'installation de Deployment Primer sur un ordinateur cible Windows requiert les actions suivantes :

- Mettez le support d'installation (DVD) Client Automation à disposition sur l'ordinateur cible ou copiez manuellement le fichier de configuration du logiciel d'injection sur l'ordinateur cible.

  Le fichier de configuration du logiciel d'injection est stocké sur le support d'installation comme suit :
  `\WindowsProductFiles_x86\DMPrimer\dmsetup.exe`

- Exécutez dmsetup.exe sur l'ordinateur cible pour installer le logiciel d'injection.

Installation de Deployment Primer sous Linux ou UNIX

L'installation de Deployment Primer sur un ordinateur cible Linux ou UNIX requiert les actions suivantes :

- Mettez le support d'installation (DVD) Client Automation à disposition sur l'ordinateur cible ou copiez manuellement l'image d'installation du logiciel d'injection sur l'ordinateur cible.

  L'image d'installation du logiciel d'injection est stockée dans le répertoire suivant du support d'installation :

  `/LinuxProductFiles_x86/dmprimer`

- Modifiez le répertoire contenant l'image d'installation du logiciel d'injection sur l'ordinateur cible et exécutez la commande d'installation suivante afin d'installer le logiciel d'injection :

  `# sh installdmp`

Spécification du certificat de gestion des déploiements lors de l'installation d'un logiciel d'injection

Le gestionnaire de déploiement génère un certificat que vous devez transférer vers l'ordinateur cible afin que le logiciel d'injection sur l'ordinateur cible accepte les packages de déploiement. Le fichier de certificat de déploiement est appelé dmkeydat.cer.

Vous pouvez choisir un autre emplacement pour le certificat lors de l'installation. Vous pouvez configurer un autre emplacement de fichier si vous voulez stocker le certificat dans une zone plus sûre, ou à un emplacement partagé entre deux gestionnaires qui fournissent une solution de basculement. Dans ce dernier cas, le partage du certificat permet aux gestionnaires de déploiement de communiquer avec les composants DMPrimer livrés par l'un des gestionnaires, sans avoir à fournir de nouveau les informations d'identification pour l'authentification.

Sous Windows, le certificat de déploiement est stocké dans le répertoire suivant :

`\Program Files\CA\DSM\DMDeploy`

Vous devez copier le certificat dans le dossier d'installation du logiciel d'injection de l'ordinateur cible. Il s'agit, par défaut, du dossier suivant :

`\Program Files\CA\DSM\DMPrimer`

Sous Linux et UNIX, le certificat de déploiement est stocké dans le répertoire suivant :

`/opt/CA/DSM/DMDeploy`

Vous devez copier le certificat dans le dossier d'installation du logiciel d'injection de l'ordinateur cible. Il s'agit, par défaut, du dossier suivant :

`/opt/CA/DSM/dmprimer/bin`

Déploiement des packages d'agent

Pour réduire le volume des données transférées via le réseau pendant le déploiement d'agents Client Automation, Client Automation fournit des packages d'agent prenant en charge l'anglais uniquement et des packages contenant des agents pour toutes les langues prises en charge (packages d'agent multilingue).

Sur le DVD d'installation du produit, les différent packages d'agent sont placés sous les dossiers de fichiers de produit, par exemple, WindowsProductFiles_x86.

Les packages en anglais uniquement possèdent le suffixe _ENU. Les packages d'agent multilingues n'ont pas de suffixe spécifique.

Dans la bibliothèque de packages logiciels, les packages ENU sont suivis de la mention "(Disponible en anglais uniquement)", tandis que les packages d'agents multilingues ne présentent aucune mention particulière.

Dans l'assistant Déploiement de l'infrastructure, les packages ENU sont identifiés par la mention "(disponible en anglais uniquement) ENU", alors que les packages multilingues incluent le suffixe NLS (ENU, DEU, FRA, JPN).

Pendant l'installation, vous pouvez choisir d'importer les packages en anglais uniquement, les packages d'agents multilingues ou les deux dans la bibliothèque Software Delivery et le dossier du package de déploiement de l'infrastructure.

Si vous sélectionnez un seul type de package, les packages en anglais par exemple, et si vous décidez ultérieurement d'ajouter les packages d'agent multilingues, vous devez exécuter une nouvelle fois la commande dsmPush pour copier le package d'agent souhaité.

Aucune langue fixe n'est spécifiée pour les déploiements d'agents multilingues vers des ordinateurs cibles. En effet, l'installation est effectuée dans la langue du système de l'ordinateur cible. Pour spécifier une langue d'installation explicite lors du déploiement sur des ordinateurs cibles, entrez l'option DSM_LANGUAGE dans le champ de saisie "Spécifiez les éventuelles options d'installation supplémentaires" de l'assistant Déploiement de l'infrastructure. L'option doit être spécifiée de la façon suivante (*lang* indique la langue d'installation sur l'ordinateur cible et correspond à enu, deu, fra, jpn, chs, esn ou kor) :

DSM_LANGUAGE=*lang* (sous Windows)

/RDSM_LANGUAGE=*lang* (sous Linux et UNIX)

Si vous ne configurez pas de paramètre linguistique, l'environnement linguistique par défaut du système est utilisé, à condition qu'un package linguistique soit disponible. Si l'environnement linguistique par défaut du système ne figure pas parmi les langues prises en charge, le programme d'installation repasse à enu (anglais (Etats-Unis)).

Lorsque vous déployez des packages sur des ordinateurs cibles à l'aide de la ligne de commande dmsweep, vous pouvez également ajouter des paramètres de langue. Il vous suffit de spécifier la langue à utiliser pour l'utilisation de Client Automation à l'aide de l'option pparams.

Exemple : déploiement d'un agent Windows en allemand à l'aide de la ligne de commande

Dans cet exemple, l'agent Windows en allemand correspond au package numéro 3.

```
dmsweep deploy /ip targetcomputer /pn 3 /pparams servername,/DSM_LANGUAGE=deu
```

Remarque : Pour plus d'informations sur les options d'installation supplémentaires (appelées également propriétés) telles que DSM_LANGUAGE, et leurs valeurs, reportez-vous aux sections concernant l'installation de Client Automation à l'aide de la ligne de commande dans le chapitre "Installation de Client Automation".

Par défaut, tous les packages d'agent sont installés dans le même mode FIPS que le gestionnaire. Vous pouvez remplacer la valeur par défaut au moyen du paramètre suivant :

Ordinateurs cibles Windows :

```
FIPS_MODE=1 //(FIPS-preferred)
FIPS_MODE=2 //(FIPS-only)
```

Ordinateurs cibles Linux ou UNIX :

```
/RITCM_FIPS_MODE=1 //(FIPS-preferred)
/RITCM_FIPS_MODE=2 //(FIPS-only)
```

Déploiement vers des ordinateurs Windows Vista et vers Windows 2008

Si le pare-feu d'un ordinateur cible exécutant le système d'exploitation Windows Vista ou Windows 2008 est désactivé et que le déploiement vers l'ordinateur échoue, vous devez créer ou définir la variable de registre suivante avec la valeur 1 :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
        System\LocalAccountTokenFilterPolicy
```

Cette opération est nécessaire, car le contrôle de compte d'utilisateur (UAC) dans Windows Vista ou Windows 2008 n'octroie pas automatiquement des droits administratifs aux utilisateurs locaux. Cela se produit même si les utilisateurs locaux sont membres du groupe Administrateurs.

Remarque : Si vous configurez cette valeur, cela désactivera le filtrage du jeton d'accès à distance de l'UAC.

Il s'avère utile de configurer cette valeur si l'utilisateur dispose d'un compte d'administrateur local sur l'ordinateur exécutant Windows Vista ou Windows 2008. Les administrateurs de domaine ne bénéficieront pas de cette modification.

Si le pare-feu d'un ordinateur cible exécutant Windows Vista ou Windows 2008 est activé, les ports suivants doivent être ouverts en plus des ports de partage de fichiers, afin de permettre le déploiement vers cet ordinateur :

- Ports UDP :

4104	CAM
137, 138	Partage de fichiers et des imprimantes, etc.

- Ports TCP :

135	dmdeploy
139, 445	Partage de fichiers et des imprimantes, etc.

Si le déploiement échoue toujours, les règles de sortie suivantes du pare-feu Windows Vista ou Windows 2008 doivent être totalement activées :

- Assistance à distance
- Détection du réseau
- Partage des fichiers et des imprimantes
- Mise en réseau du noyau

Si après avoir ouvert les ports et activé les règles de sortie, l'analyse de déploiement ne renvoie toujours pas de réponse, vous devrez définir l'option de configuration "Ne pas exécuter la commande ping sur la cible lors d'une analyse" sur True. Cette option se trouve dans la stratégie de configuration, à la section Gestionnaire\Déploiement de l'infrastructure. Cette option marque la cible avec "Réponse de l'ordinateur en cours" lors d'une analyse et permet la poursuite du déploiement. Bien que cela ne garantisse pas la réussite du déploiement, cette méthode permet de contourner les problèmes pouvant survenir lors de la mise en contact initiale de l'ordinateur cible.

Déploiement à l'aide de l'explorateur DSM

L'assistant Déploiement de l'infrastructure aide les administrateurs à déployer les agents ou serveurs de modularité au sein de leur entreprise.

L'assistant vous guide étape par étape dans le processus de création d'un job de déploiement. Vous pouvez choisir deux types de jobs : Déployer le logiciel vers des ordinateurs cibles et Transférer des packages vers le serveur de modularité. Vous sélectionnez le package à déployer dans une liste, puis vous spécifiez s'il doit être déployé vers un ordinateur spécifique ou vers tous les ordinateurs dans un domaine spécifique, au sein d'une plage d'adresses IPv4 ou d'un répertoire. Ensuite, l'assistant analyse les ordinateurs cibles pour savoir si le déploiement est possible sur toutes les cibles et si des informations d'identification sont requises pour le déploiement.

L'assistant affiche des descriptions à l'écran pour chaque étape et un système d'aide distinct.

Après le début du job de déploiement, vous pouvez le surveiller et le contrôler via la fonction Etat du job de déploiement dans le Panneau de configuration. Pour plus d'informations, consultez la section Surveillance et contrôle des jobs de déploiement d'agents de l'*Aide de l'explorateur DSM*.

Remarque : Lors de l'installation des packages de modules d'extension de l'agent sur des ordinateurs en zone non globale sous Solaris, le message suivant peut s'afficher dans le volet Etat du job de déploiement : "Echec d'installation de dmprimer par SSH". Pour résoudre ce problème, mettez à jour l'adresse IP de l'agent et son nom dans le fichier hosts (/etc/hosts).

Déploiement en utilisant la ligne de commande

L'utilitaire dmsweep vous permet d'automatiser les activités de déploiement et d'exécuter de manière interactive un grand nombre des tâches identiques à celles de l'explorateur DSM.

Deployment Management fournit l'autorisation d'installer l'agent DMPrimer via dmsweep, dans les environnements Windows NT, comme indiqué ci-dessous. L'utilitaire dmsweep se connecte au gestionnaire de déploiement en utilisant des mécanismes de sécurité standard. En tant qu'utilisateur de dmsweep, l'administrateur système doit vous octroyer la capacité d'effectuer des déploiements vers le gestionnaire (les administrateurs disposant de privilèges au niveau du système d'exploitation disposent par défaut des privilèges de déploiement). Vous pouvez préciser les informations d'identification de l'ordinateur cible en utilisant les arguments /tu (nom d'utilisateur) et /tp (mot de passe).

Déploiement déclenché par la détection continue

La fonction permettant de déployer des logiciels dès que de nouveaux systèmes sont détectés est basée sur la fonction Détection continue de CA Common Services. L'agent DIA (agent d'intelligence distribuée) de CA Common Services sert à extraire des événements à chaque détection d'un nouveau système. La fonctionnalité Détection continue est activée dès que l'utilisateur a créé au moins une stratégie, afin de décrire quel package est supposé être déployé vers quel ordinateur cible en fonction de l'adresse IPv4 et du système d'exploitation de l'ordinateur. Les stratégies peuvent être définies dans l'assistant Stratégie de déploiement de détection continue, ce qui s'apparente à l'assistant Déploiement de l'infrastructure.

Le processus de détection se présente comme suit :

- Un système se connecte au réseau pour la première fois.
- Le service Détection continue détecte le nouveau matériel, puis, à l'aide de ses heuristiques, le classifie et crée un objet géré qui représente le système dans le référentiel WorldView.
- En réponse aux nouvelles données qui arrivent dans la base de données, un déclencheur est exécuté et enregistre l'événement dans une table d'événements (dédie) spéciale.
- L'application de détection Client Automation enregistrée pour ces événements est notifiée.
- L'application de détection vérifie les stratégies de détection continue pour savoir si le système détecté est ciblé afin de recevoir de nouveaux logiciels, puis appelle l'interface de déploiement d'une manière similaire à celle de DMSweep.

Remarque : Pour permettre le bon fonctionnement de la détection continue, configurez le port Microsoft SQL Server sur le port par défaut 1433 dans le gestionnaire de domaines.

Packages de déploiement

Les types de packages de déploiement suivants sont proposés :

- Agent CA DSM + module d'extension d'inventaire de base
- Agent CA DSM + module d'extension Asset Management
- Agent CA DSM + module d'extension Remote Control
- Agent CA DSM + module d'extension Software Delivery
- Agent CA DSM + module(s) d'extension AM, RC, SD

  Ce package comporte les modules d'extension d'agent d'inventaire de base, Asset Management, Remote Control et Software Delivery.

  Pour Linux, ce package inclut également le module d'extension de l'agent de transport de données.

- Serveur de modularité CA DSM

  Ce package combiné contient les modules d'extension d'agent et de serveur de modularité pour Basic Inventory, Asset Management, Remote Control, Software Delivery et Data Transport CA.

  Remarque : Lorsque le package de déploiement Serveur de modularité CA DSM est déployé à l'aide de DMDeploy, le module d'extension de serveur de modularité et *tous* les modules d'extension de l'agent sont installés. Cependant, lorsque ce package est déployé à l'aide de la fonctionnalité de livraison de logiciels, seuls le module d'extension de serveur de modularité et les modules d'extension de l'agent Software Delivery et de l'agent de transport de données CA sont installés.

  Remarque : Pour obtenir des informations sur le package de déploiement du serveur de modularité CA DSM Linux (Intel), reportez-vous à la section Installation du serveur de modularité sous Linux (page 157).

- Pour déployer l'analyseur de conformité des unités (DCS), utilisez les packages de déploiement suivants :

  Windows

  - Module d'extension AM DCS de l'agent CA DSM (disponible en anglais uniquement)
  - Module d'extension AM DCS de l'agent CA DSM

- Pour déployer l'inventaire à distance des systèmes virtualisés, utilisez les packages de déploiement suivants :

  Windows

  - Module d'extension AM RVI de l'agent CA DSM (disponible en anglais uniquement)
  - Module d'extension AM RVI de l'agent CA DSM

  AIX

- Module d'extension AM RVI de l'agent CA DSM AIX (RS/6000) (ENU)

HP-UX

- Module d'extension AM RVI de l'agent CA DSM HP-UX (RS/800) (ENU)

Linux

- Module d'extension AM RVI de l'agent CA DSM Linux (intel) (ENU)

Solaris SPARC

- Module d'extension AM RVI de l'agent CA DSM Solaris SPARC (ENU)

Remarque : Aucune documentation Client Automation n'est installée avec les packages client déployés.

Les packages de déploiement se trouvent sur un ordinateur du gestionnaire uniquement si la fonction de gestionnaire pour le déploiement est installée sur le système local (valeur par défaut).

Vous pouvez modifier l'emplacement par défaut pour les packages de déploiement lors de la phase interactive de l'installation.

Important : Vous pouvez spécifier des propriétés de ligne de commande MSI supplémentaires pour les versions Windows des packages de déploiement, mais faites attention aux versions Windows des packages "Agent CA DSM + module(s) d'extension AM, RC, SD" et "Serveur de modularité CA DSM". Pour ces packages MSI combinés, vous ne devez pas spécifier de propriétés de la liste de fonctions MSI spécifiques au package, telles que ADDLOCAL ; dans le cas contraire, le déploiement du package échouera. Si vous devez répertorier des fonctions spécifiques à un package, nous vous recommandons de le faire pour le package de déploiement en question de l'agent dédié.

Outil dsmpush

L'outil (script) dsmpush vous permet d'importer ou de "pousser" les packages d'installation du DVD d'installation sur le gestionnaire de domaine. L'outil dsmpush sert à importer des packages adaptés à l'utilisation par la fonction Déploiement de l'infrastructure ou Software Delivery.

Normalement, les packages sont déjà placés sur un ordinateur gestionnaire pendant l'installation, mais ce placement est facultatif. Si vous devez replacer les packages, ajouter d'autres packages ou mettre à jour les packages, vous pouvez utiliser l'outil dsmpush.

L'outil dsmpush offre une fonction de vérification et de copie. La fonction de copie valide et répertorie les packages de déploiement existants dans le gestionnaire. La fonction de copie permet d'importer un ensemble de packages pour des produits et systèmes d'exploitation spécifiés dans une bibliothèque de déploiement de l'infrastructure sur votre système local ou dans une bibliothèque Software Delivery.

A chaque exécution, l'outil dsmpush fournit des informations de journalisation dans le fichier journal TRC_Inst_dsmPush.*jjmmaaahhmmss*.log, dans lequel *jjmmaaahhmmss* est l'horodateur du fichier journal.

Pour obtenir une description des fonctions de contrôle et de copie de dsmpush ainsi que de leurs paramètres, consultez le *Manuel de référence des composants CLI*.

Conditions préalables pour le déploiement automatique de l'infrastructure Client Automation

Le composant Déploiement de l'infrastructure vous permet d'installer à distance le logiciel de l'agent et du serveur de modularité sur des ordinateurs cibles n'exécutant pas le logiciel Client Automation. Cette installation peut uniquement être obtenue en utilisant les fonctionnalités proposées par les systèmes d'exploitation sous-jacents sur les ordinateurs source et cible ; elle est soumise aux restrictions imposées par la configuration réseau de l'entreprise.

L'étape initiale lors du déploiement du logiciel d'infrastructure consiste à installer à distance un petit logiciel d'injection, DMPrimer, sur l'ordinateur cible. Ce logiciel DMPrimer est chargé du transfert ultérieur des images d'installation du composant logiciel d'infrastructure et de l'invocation de leur installation. Lors de la distribution du DMPrimer sur les ordinateurs cibles, le gestionnaire de déploiement doit fournir des informations d'identification utilisateur valides sur la cible.

Le DMPrimer est transféré sur le système cible en utilisant l'un des mécanismes suivants. Si le gestionnaire du déploiement connaît le système d'exploitation de l'ordinateur cible, un mécanisme de transfert adapté est sélectionné. Si le système d'exploitation cible ne peut être déterminé, chacun des mécanismes suivant est tenté à tour de rôle.

- **Ouverture d'un partage réseau**

  Le gestionnaire de déploiement tente de se connecter au partage réseau Windows sur le système cible. Par défaut, le nom de partage utilisé est ADMIN$; cependant, cela peut être modifié à l'aide de la stratégie de configuration "defaultTargetShare". Ce mécanisme est disponible uniquement à partir des gestionnaires de déploiement s'exécutant sur une plate-forme basée sur Windows et ne fonctionnera que sur certaines cibles Windows. Des variantes de Windows, par exemple Windows XP Edition Familiale, ne prennent pas en charge ce mécanisme de déploiement.

- **Ouverture d'une connexion réseau vers l'ordinateur cible en utilisant le protocole SSH et transfert du package d'installation du Primer en utilisant SFTP**

  Ce mécanisme fonctionne sur tout ordinateur exécutant un serveur SSH ; cependant, il est principalement utilisé pour le ciblage d'ordinateurs Linux ou UNIX.

  Remarque : Lorsque vous effectuer un déploiement sur des systèmes Solaris, CA recommande d'utiliser SunSSH v1.1 ou ultérieure, ou la dernière version d'OpenSSH. Pour des informations complémentaires sur les patchs applicables aux plates-formes Solaris et aux versions, consultez le site http://opensolaris.org/os/community/security/projects/SSH.

  Si vous exécutez un pare-feu sur l'ordinateur cible, assurez-vous que le port SSH (22) est activé pour autoriser la connexion depuis le gestionnaire de déploiement. Vous devez également vérifier que le serveur SSH sur l'ordinateur cible est configuré pour utiliser une clé RSA ainsi que le chiffrement 3DES et le code d'authentification de message (MAC) HMAC-SHA1. La plupart des serveurs SSH prennent en charge cette configuration par défaut, mais dans le cas contraire, vous devez consulter la documentation de votre serveur SSH pour savoir comment l'ajouter.

  Important : Sur Solaris 11, les chiffrements par défaut pour sshd sont aes128-ctr, aes192-ctr, aes256-ctr, arcfour128, arcfour256 et arcfour. Le déploiement requiert 3DES, vous devez donc ajouter les chiffrements 3des-cbc au fichier de configuration sshd et redémarrez le sshd.

  Pour déployer vers un agent UNIX ou Linux, effectuez les modifications suivantes dans le fichier de configuration /etc/ssh/sshd_config de votre nouvelle implémentation de SSH :

  - Définissez PasswordAuthentication sur Yes.
  - Définissez PermitRootLogin sur Yes.
  - Vérifiez que le sous-système SFTP est activé.

  Lors du déploiement vers certains systèmes AIX IBM exécutant à la fois la pile IPv4 et IPv6 et utilisant une adresse IPv6, le serveur SSH de l'ordinateur cible risque d'écouter uniquement sur le port 22 pour IPv4. Cela fera échouer le déploiement. Pour corriger ce problème, modifiez le fichier de configuration sshd_config et définissez le paramètre ListenAddress sur "::".

  Lorsque vous effectuez un déploiement sur Solaris 11, procédez comme suit :

  - Mettez la ligne suivante en commentaire :

    ```
    CONSOLE=/dev/console
    ```

  - en commentaire :

    ```
    /etc/default/login.
    vi /etc/default/login
    #CONSOLE=/dev/console
    ```

  - Supprimez l'élément suivant de l'entrée racine dans /etc/user_attr :

```
;type=role
```

ou utilisez la commande :

```
rolemod -K type=normal root
```

- Redémarrez le service SSH.

Remarque : Si vous voulez que la communication SSH entre le gestionnaire de déploiement et l'ordinateur cible soit conforme à la norme FIPS, vous devez vérifier que le serveur SSH en cours d'exécution sur la cible utilise aussi un module cryptographique conforme à la norme FIPS et définir le mode FIPS uniquement au niveau du gestionnaire de déploiement.

- **Ouverture d'une connexion réseau vers l'ordinateur cible à l'aide du protocole Telnet et transfert de l'installation du logiciel d'injection à l'aide du FTP**

  Ce mécanisme est principalement utilisé pour le ciblage de systèmes UNIX ne prenant pas SSH en charge. L'utilisation de Telnet/FTP est moins répandue en raison des failles de sécurité inhérentes à ces protocoles ; elle est remplacée par l'utilisation de SSH/SFTP.

  Lors de l'utilisation de cette méthode de connexion, des commandes Telnet, exécutées sur des ordinateurs cibles, extraient l'image d'installation de DMPrimer à partir d'un serveur FTP situé dans le gestionnaire.

Important : Certains systèmes d'exploitation modernes n'encouragent pas l'installation à distance de logiciels, voire l'interdisent activement. Si vous tentez de déployer le logiciel Client Automation sur de tels systèmes, vous constatez généralement l'échec du déploiement avec un état "Absence de transport de logiciel d'injection". Dans ce cas, l'installation des composants logiciels Client Automation peut être effectuée par d'autres moyens, par exemple l'installation à partir de supports de distribution physique tels que le DVD.

Vous pouvez également installer le logiciel DMPrimer manuellement. Cela permet de déployer l'infrastructure Client Automation sans devoir dépendre des fonctionnalités offertes par les systèmes d'exploitation sous-jacents.

Pour savoir si un déploiement automatique est possible dans votre environnement, vous pouvez procéder à quelques vérifications simples en exécutant les opérations du système d'exploitation standard suivantes :

- Pour la livraison de l'image DMPrimer à l'aide de partages Windows, vous devez être en mesure de créer un mappage à un partage (par défaut : ADMIN$) à partir de l'ordinateur hôte de votre gestionnaire de déploiement vers chaque ordinateur cible de déploiement, à l'aide des informations d'identification d'utilisateur cible fournies dans la demande de déploiement.
- Pour la livraison de l'image DMPrimer à l'aide de SSH, vous devez pouvoir vous connecter avec SSH à partir du gestionnaire de déploiement aux ordinateurs cibles de déploiement.
- Pour la livraison de DMPrimer à l'aide de Telnet, vous devez pouvoir vous connecter avec un client Telnet à vos ordinateurs cibles de déploiement, à l'aide des informations d'identification racine/Administrateur fournies dans la demande de déploiement. Vous devez également être en mesure d'effectuer une opération d'extraction FTP à partir d'ordinateurs cibles de gestionnaire, en vous connectant à FTP en tant qu'utilisateur anonyme.

Modification des détails du serveur FTP pour une utilisation avec le Déploiement de l'infrastructure

Les détails facultatifs concernant le serveur FTP utilisés pour stocker des packages de déploiement de l'infrastructure peuvent être modifiés une fois l'installation terminée, par exemple si vous voulez déplacer des packages FTP sur un autre serveur.

Pour modifier les détails facultatifs sur un ordinateur cible Windows, exécutez la commande suivante :

```
\Program Files\CA\DSM\bin\dmdeploy.exe ftpinfo Serveur_FTP Utilisateur_FTP
MotDePasse_FTP
```

Serveur_FTP

Indique l'adresse de l'ordinateur qui héberge le serveur FTP.

Utilisateur_FTP

Spécifie l'utilisateur pour se connecter à FTP.

MotDePasse_FTP

Spécifie le mot de passe associé à l'utilisateur FTP.

Paramètres Windows XP pour activer Agent Deployment

Pour activer le déploiement d'agents vers des ordinateurs cibles qui exécutent un logiciel pare-feu, Windows Firewall sous Windows XP Professional SP2 par exemple, vous devez réaliser manuellement les actions suivantes :

1. Modifiez la stratégie de sécurité "Accès réseau : modèle de partage et de sécurité pour les comptes locaux" de "Invité uniquement - Utilisateurs locaux authentifiés en tant qu'Invités" à "Classique - Utilisateurs locaux authentifiés en tant qu'utilisateurs locaux" (s'applique à Windows XP).

   Le modèle Classique permet un contrôle étroit de l'accès aux ressources et empêche les connexions au réseau par le biais de comptes locaux d'être mappées sur le compte Invité, qui a normalement uniquement un accès en "Lecture seule" à une ressource donnée.

   Pour obtenir de plus amples informations, consultez la page Web Accès réseau : modèle de partage et de sécurité pour les comptes locaux de la documentation du produit Windows.

2. Configurez les paramètres de pare-feu suivants.

   - Autoriser le partage des fichiers et des imprimantes
   - Ouvrir le port UDP 4104
   - Ouvrir le port TCP 135

Chapitre 6: Remarques sur la migration et la mise à niveau

Ce chapitre traite des sujets suivants :

Chemins de mise à niveau pris en charge

Client Automation Version 12.9 prend en charge les mises à niveau des produits et des versions suivantes :

- Pour les composants de gestionnaire, la mise à niveau est prise en charge depuis :
  - Client Automation 12.5 SP1
  - Client Automation 12.5 SP1 C1
  - Client Automation 12.8
  - Client Automation 12.8.01 Feature Pack
- Pour le serveur de modularité et les composants d'agent, la mise à niveau est prise en charge à partir de :
  - Client Automation 12.5 SP1
  - Client Automation 12.5 SP1 C1
  - Client Automation 12.8
  - Client Automation 12.8.01 Feature Pack

Remarques générales

Toutes les mises à niveau doivent être effectuées sur une base de langue similaire. Par exemple, vous pouvez effectuer une mise à niveau de la version française de Client Automation vers la version française de Client Automation, mais pas vers la version anglaise.

Remarques concernant la mise à niveau des composants Client Automation

Lors de la mise à niveau des composants Client Automation, prenez en compte ce qui suit :

- Les nouvelles signatures forcées par le serveur de modularité Client Automation Version 12.9 pour détecter les images d'application virtualisée sont étiquetées de façon spéciale, et sont, pour cette raison, ignorées par les agents hérités.

Considérations relatives à MDB

Vous devez prendre en compte les remarques suivantes concernant la norme MDB :

- Client Automation Version 12.9 ne prend pas en charge les MDB Microsoft SQL Server 2005. Mettez le système de gestion de bases de données à niveau vers Microsoft SQL Server 2008 ou une version ultérieure avant de procéder à la mise à niveau vers Client Automation Version 12.9.

Remarques concernant les mises à niveau

Lorsque vous procédez à la mise à niveau vers la Version 12.9 :

- Client Automation met à niveau les composants qui sont installés avec la version précédente uniquement. Pour installer les composants de la version actuelle ou des composants supplémentaires, exécutez le programme d'installation avec l'option modify et sélectionnez les composants pour l'installation. Par exemple, Migration automatisée et Collecteur d'alertes.
- Si la console d'administration Web est configurée avec SSL avant la mise à niveau, veillez à importer les certificats vers le magasin de certificats JRE 1.7 à l'issue de la mise à niveau. Pour plus de détails, consultez la rubrique Activation de SSL pour la console Web et les services Web dans l'Aide de la console Web.
- Lorsque les agents CA Asset Management ou CA Remote Control sous Windows sont mis à niveau via un job de livraison de logiciels, le package de l'agent Software Delivery est ajouté automatiquement à ce job. L'agent Software Delivery est d'abord mis à niveau, suivi par les agents demandés.
- Lors de la mise à niveau des composants IPS OSIM, vérifiez que la sauvegarde d'un fichier template.ini personnalisé est disponible avant le placement de la dernière version du fichier template.ini dans le répertoire d'installation OSIM. Appliquez tout changement personnalisé de la sauvegarde de template.ini au nouveau template.ini. Dans les versions ultérieures, Client Automation contiendra des mises à jour d'outils extensibles pour la prise en charge de la personnalisation du boiler template.ini.
- Pour que les modules d'extension fonctionnent correctement, mettez à niveau tous les modules d'extension de DSM vers la version actuelle.

Informations de mise à niveau

Remarque : Lorsque vous procédez à la mise à niveau à partir de Client Automation r12.5 SP1 ou r12.5 SP1 C1, CCS n'est pas mis à niveau. La version actuelle contient des patchs de CCS supplémentaires requis pour la prise en charge de Windows Server 2012 et SQL Server 2012. Si vous souhaitez mettre à niveau les ordinateurs de gestionnaire vers Windows Server 2012 ou SQL Server 2012, contactez le support technique de CA pour obtenir la liste des patchs à appliquer.

Pendant la mise à niveau à partir des versions 12.5 SP1 et 12.5 SP1C1 vers *Client Automation Version 12.9, n'exécutez pas la commande caf kill all avant la fin de la mise à niveau. Exécutez la commande caf stop, lorsqu'elle est requise.*

Considérations relatives à la norme FIPS

Vous devez prendre en compte les remarques suivantes concernant la norme FIPS :

- Vous pouvez sélectionner le mode FIPS pendant une installation personnalisée uniquement. L'installation expresse installe toujours Client Automation dans le mode Préférence-FIPS. Dans le cas d'une installation d'un agent Remote Control autonome, vous pouvez spécifier le mode FIPS, que l'installation soit personnalisée ou expresse.
- Tous les composants mis à niveau utilisent le mode Préférence FIPS jusqu'à ce que vous les basculiez explicitement vers le mode FIPS uniquement. Vous pouvez passer en mode FIPS uniquement lorsque vous avez procédé à la mise à niveau vers la version actuelle de tous les composants de l'infrastructure Client Automation. Pour plus d'informations sur le passage d'un mode FIPS à un autre, consultez la section Fonctionnalités de sécurité.
- Après avoir mis à niveau le gestionnaire de domaines et le système de préparation d'images (IPS), vous pouvez utiliser ce dernier pour mettre à niveau le système d'exploitation et les images de démarrage existants afin de les rendre conformes aux normes FIPS. Vous pouvez alors enregistrer et appliquer les images migrées aux serveurs de démarrage. Pour plus d'informations sur la mise à niveau, l'enregistrement et l'application des images de SE, consultez le *Manuel d'administration du système de gestion des installations de systèmes d'exploitation*.

Informations complémentaires :

Passage en mode FIPS uniquement (page 455)
Passage en mode Préférence FIPS (page 456)

Remarques sur la mise à niveau du système OSIM

Lors de la mise à niveau de CA ITCM R12.5 SP1 FP1 patch CentOS (R055831) ou R12.5 SP1 FP1 C1 vers Client Automation Version 12.9, effectuez les opérations suivantes :

- Mettez à jour l'image de démarrage basée sur Linux (LinuxPE).
- Mettez à jour les images de SE RHEL5.x et RHEL6.x existantes basées sur LinuxPE.
- Mettez à jour toutes les images de SE existantes (précédemment prises en charge par WinPE et DOSx) désormais prises en charge par LinuxPE. Après avoir mis à jour l'image de SE existante, vérifiez que la valeur du paramètre de démarrage InstallDrive est sda, sdb.
- Remplacez la valeur manuellement par celle prise en charge par les images de SE.

Remarque : Spécifiez le paramètre de démarrage InstallDrive relatif à l'utilisation du disque local pour l'installation de système d'exploitation. La valeur par défaut est vide et le premier disque local disponible est utilisé pour l'installation du système d'exploitation.

Pour ajouter un disque, procédez comme suit :

- Ajoutez les disques à partir de l'explorateur DSM, comme *sde, sdf* pour plus de quatre disques.
- Modifiez le fichier OS.def sous le dossier du système de préparation d'images OSIM : CA\DSM\osimips\os-template\camenu.

Tenez compte de la nouvelle définition pour le paramètre de démarrage InstallDrive pour les images de SE LinuxPE :

```
[InstallDrive]

Type=MapListExt

Trans=yes

MaxLength=128

Comment=Disque sur lequel installer le système d'exploitation, comme sda, sdb ou sdc.

item=sda

item=sdb

item=sdc

item=sdd
```

Pour plus d'informations, reportez-vous au Manuel d'administration de la gestion des installations de systèmes d'exploitation.

Processus de mise à niveau

La mise à niveau de Client Automation est un processus qui peut prendre du temps et qui peut être affecté par de nombreux facteurs externes, tels que le manque de ressources système ou les coupures de courant inattendues. Pour éviter les pertes de données, nous vous conseillons d'effectuer une sauvegarde complète de votre installation avant de procéder à toute mise à niveau, en particulier celle des composants de gestionnaire et de serveur de modularité.

L'ordre d'exécution des mises à niveau des composants est capital. Cette version de Client Automation prend en charge une stratégie de mise à niveau strictement décroissante. Avant de poursuivre, étudiez intégralement les phases et étapes ci-dessous.

- Phase 1 : mise à niveau du gestionnaire d'entreprise DSM
- Phase 2 : mise à niveau du gestionnaire d'entreprise DSM
- Phase 3 : mise à niveau des serveurs de modularité DSM
- Phase 4 : mise à niveau des agents DSM

Après chaque phase de mise à niveau, la configuration est entièrement fonctionnelle. En d'autres termes, les composants qui ont été mis à niveau peuvent communiquer avec des composants qui ne l'ont pas encore été.

Remarque : Lorsque vous utilisez le DVD d'installation Client Automation pour mettre à niveau le logiciel Client Automation précédemment installé sur un ordinateur, vous devez prendre en compte le fait que tous les composants Client Automation installés sur cet ordinateur seront mis à niveau.

Remarque : Si vous essayez de mettre à niveau votre installation existante à partir d'une source ou d'un support d'installation (lecteur DVD, par exemple) autre que celui utilisé pour l'installation Unicenter DSM d'origine, l'installation de la mise à niveau peut échouer avec le code d'erreur MSI 1602. Pour éviter cela, il est recommandé de configurer votre installation pour qu'elle utilise la même source ou le même support que pour l'installation d'origine.

Remarques importantes sur la mise à niveau

- Il n'est pas possible de modifier la langue d'une installation existante lors d'une mise à niveau. Si vous spécifiez un identificateur de langue différent, par exemple, dans le fichier de réponses pour une mise à niveau effectuée en mode autonome, la mise à niveau est abandonnée.
- Une fois le gestionnaire de domaines de DSM mis à niveau, dans l'explorateur DSM, accédez à Panneau de Configuration, Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Gestionnaire, Déploiement de l'infrastructure et vérifiez que la valeur du paramètre Toujours déployer un logiciel d'injection est défini sur False.

  Lorsque la valeur de paramètre est définie sur False, le gestionnaire met uniquement à niveau le DMPrimer sur les ordinateurs cibles disposant d'une version antérieure à celle du gestionnaire. Si vous définissez le paramètre sur True, le gestionnaire met à niveau le DMPrimer des ordinateurs cibles, quelle que soit la version.
- Pendant la mise à niveau, les certificats ne sont pas mis à jour afin de préserver les certificats personnalisés existants qui peuvent déjà se trouver sur l'ordinateur. Si l'image principale a été mise à jour pour utiliser de nouveaux certificats personnalisés, ces derniers sont copiés dans le dossier bin pendant l'installation, mais ne sont pas appliqués au magasin de certificats.

  Les certificats personnalisés doivent être appliqués pendant les installations initiales ou appliqués manuellement après le processus de mise à niveau. Les commandes nécessaires à l'importation de nouveaux certificats sont détaillées dans la section Authentification (page 407) du chapitre Fonctionnalités de sécurité.

Phase 1 : Mise à niveau du gestionnaire d'entreprise DSM

Au cours de la phase 1 du processus de mise à niveau, vous mettez à niveau le gestionnaire d'entreprise DSM. En général, les gestionnaires d'entreprise ne sont installés que dans de très grandes entreprises ou dans des entreprises réparties sur plusieurs sites. Si vous installez un gestionnaire d'entreprise DSM pour la première fois, passez à la phase 2 de la mise à niveau.

Pour mettre à niveau le gestionnaire d'entreprise, procédez comme suit :

1. Fermez tous les services et toutes les applications connectés à la MDB d'entreprise DSM.

   Par exemple, dans le cas d'une implémentation de Client Automation simple, fermez le gestionnaire d'entreprise DSM, les moteurs distants de gestionnaires d'entreprise et de domaines, ainsi que les instances du générateur de rapports DSM en cours d'exécution. Vous devrez également fermer toutes les applications CA ou autres produits tiers de votre réseau qui partagent la MDB et y sont connectées.

2. Si nécessaire, mettez à niveau la MDB à partir du DVD.

   Si la MDB est installée sur un ordinateur distant du gestionnaire d'entreprise DSM, effectuez la mise à niveau de la MDB en utilisant le DVD Client Automation. Sélectionnez l'option Installer la MDB ou Installer CCS y compris MDB.

   Client Automation 12.9 vous permet également de mettre à niveau la MDB et le gestionnaire en une seule fois à l'aide du programme d'installation. Le programme d'installation identifie l'ordinateur de la MDB et la met à niveau, puis met à niveau le gestionnaire. Cette fonctionnalité n'est pas prise en charge si la MDB est installée à l'aide de l'option Installer CCS et la MDB.

3. A partir du DVD, mettez à niveau le gestionnaire d'entreprise DSM.

4. Si nécessaire, mettez à niveau tous les moteurs d'entreprise DSM distants à partir du DVD.

   Si vous avez déjà installé des moteurs de niveau entreprise sur des ordinateurs distants, mettez-les à niveau maintenant à l'aide du DVD Client Automation.

5. Si nécessaire, mettez à niveau tous les explorateurs DSM ou générateurs de rapports DSM distants à partir du DVD ou à l'aide du package Software Delivery.

   Toutes les instances autonomes de l'explorateur DSM, du générateur de rapports DSM, des services Web ou de la console Web utilisées pour se connecter au gestionnaire d'entreprise DSM et qui n'ont pas encore été mises à niveau lors des étapes précédentes doivent être mises à niveau maintenant. Les instances installées sur des ordinateurs également dotés d'un serveur de modularité DSM ou d'un agent DSM doivent être mises à niveau respectivement après la phase 3 et la phase 4.

Remarque : Client Automation Version 12.9 est compatible uniquement avec CA Asset Intelligence Version 12.9 ou CA Patch Manager Version 12.9. Lors de la mise à niveau de Client Automation Version 12.9, vous devez aussi mettre à niveau CA Asset Intelligence ou CA Patch Manager vers la version Version 12.9.

Remarque : Lorsque vous procédez à la mise à niveau à partir de Client Automation r12.5 SP1 ou r12.5 SP1 C1, CCS n'est pas mis à niveau. La version actuelle contient des patchs de CCS supplémentaires requis pour la prise en charge de Windows Server 2012 et SQL Server 2012. Si vous souhaitez mettre à niveau les ordinateurs de gestionnaire vers Windows Server 2012 ou SQL Server 2012, contactez le support technique de CA pour obtenir la liste des patchs à appliquer.

Pendant la mise à niveau à partir des versions 12.5 SP1 et 12.5 SP1C1 vers *Client Automation Version 12.9, n'exécutez pas la commande caf kill all avant la fin de la mise à niveau. Exécutez la commande caf stop, lorsqu'elle est requise.*

Phase 2 : Mise à niveau du gestionnaire de domaines DSM

Dans la phase 2 du processus de mise à niveau de Client Automation, vous mettez à niveau le gestionnaire de domaines.

Pour mettre à niveau le gestionnaire de domaines DSM, procédez comme suit :

1. Fermez tous les services et toutes les applications connectés à la MDB de domaines DSM.

   Par exemple, dans le cas d'une implémentation de Client Automation simple, fermez le gestionnaire de domaines DSM, les moteurs distants de gestionnaires d'entreprise et de domaines, ainsi que les instances du générateur de rapports DSM en cours d'exécution (pour ce domaine ainsi que pour le gestionnaire d'entreprise parent). Vous devrez également fermer toutes les applications CA ou autres produits tiers de votre réseau qui partagent la MDB et y sont connectées.

2. Si nécessaire, mettez à niveau la MDB à partir du DVD d'installation Client Automation.

   Si la MDB est installée sur un ordinateur distant du gestionnaire de domaines DSM, effectuez la mise à niveau de la MDB à partir du DVD d'installation. Sélectionnez l'option Installer la MDB ou Installer CCS y compris MDB.

   CA Client Automation 12.9 vous permet également de mettre à niveau la MDB et le gestionnaire en une seule fois à l'aide du programme d'installation. Le programme d'installation identifie l'ordinateur de la MDB et la met à niveau, puis met à niveau le gestionnaire. Cette fonctionnalité n'est pas prise en charge si la MDB est installée à l'aide de l'option Installer CCS et la MDB.

3. A partir du DVD d'installation, mettez à niveau le gestionnaire de domaines DSM.

4. Si nécessaire, mettez à niveau tous les moteurs de domaines DSM distants à partir du DVD d'installation.

   Si vous avez déjà installé des moteurs DSM de niveau domaine sur des ordinateurs distants, mettez-les à niveau maintenant à l'aide du DVD d'installation.

5. Si nécessaire, mettez à niveau tous les explorateurs DSM ou générateurs de rapports DSM distants à partir du DVD d'installation ou à l'aide du package Software Delivery.

   Toutes les instances autonomes de l'explorateur DSM, du générateur de rapports DSM, des services Web ou de la console Web utilisées pour se connecter au gestionnaire de domaines DSM et qui n'ont pas encore été mises à niveau lors des étapes précédentes doivent être mises à niveau maintenant. Les instances installées sur des ordinateurs également dotés d'un serveur de modularité DSM ou d'un agent DSM doivent être mises à niveau respectivement après la phase 3 et la phase 4.

Remarque : Client Automation Version 12.9 est compatible uniquement avec CA Asset Intelligence Version 12.9 ou CA Patch Manager Version 12.9. Lors de la mise à niveau de Client Automation Version 12.9, vous devez aussi mettre à niveau CA Asset Intelligence ou CA Patch Manager vers la version Version 12.9.

Remarque : Lorsque vous procédez à la mise à niveau à partir de Client Automation r12.5 SP1 ou r12.5 SP1 C1, CCS n'est pas mis à niveau. La version actuelle contient des patchs de CCS supplémentaires requis pour la prise en charge de Windows Server 2012 et SQL Server 2012. Si vous souhaitez mettre à niveau les ordinateurs de gestionnaire vers Windows Server 2012 ou SQL Server 2012, contactez le support technique de CA pour obtenir la liste des patchs à appliquer.

Pendant la mise à niveau à partir des versions 12.5 SP1 et 12.5 SP1C1 vers *Client Automation Version 12.9, n'exécutez pas la commande caf kill all avant la fin de la mise à niveau. Exécutez la commande caf stop, lorsqu'elle est requise.*

Phase 3 : Mise à niveau des serveurs de modularité DSM

Les outils suivants de mise à niveau des serveurs de modularité DSM sont à votre disposition :

- Utilisation du DVD d'installation Client Automation
- Utilisation des packages Software Delivery pour les serveurs de modularité
- Utilisation du déploiement de l'infrastructure (DMDeploy) pour les serveurs de modularité

Pour mettre à niveau les serveurs de modularité à l'aide du DVD d'installation, insérez le DVD dans l'ordinateur utilisé en tant que serveur de modularité et suivez les étapes indiquées par l'assistant d'installation interactif.

Pour mettre à niveau les serveurs de modularité à l'aide de packages Software Delivery, créez un job de déploiement Software Delivery comportant le package de serveur de modularité DSM et planifiez l'exécution du job Software Delivery sur les ordinateurs servant de serveurs de modularité.

Pour mettre à niveau les serveurs de modularité Windows à l'aide du déploiement d'infrastructure (DMDeploy), déployez le nouveau package de serveur de modularité vers les ordinateurs servant de serveurs de modularité. Cette action permet de mettre à niveau le serveur de modularité, l'agent et les modules d'extension de l'agent déjà installés. Pour que le programme d'installation mette à niveau les modules d'extension de l'agent, vous devez spécifier les paramètres suivants dans le champ Options d'installation Windows supplémentaires de l'assistant de déploiement de l'infrastructure :

REINSTALL=ALL REINSTALLMODE=vomus

Pour mettre à niveau les serveurs de modularité Linux à l'aide du déploiement d'infrastructure (DMDeploy), déployez le nouveau package de serveur de modularité vers les ordinateurs servant de serveurs de modularité. Cette action permet de mettre à niveau le serveur de modularité, l'agent et les modules d'extension de l'agent déjà installés.

Phase 4 : Mise à niveau des agents DSM

Les agents DSM peuvent être mis à niveau en utilisant l'une des techniques décrites ci-dessous. Veuillez vérifier les méthodes décrites dans la liste suivante et sélectionner la mieux adaptée. Vous trouverez la description détaillée de la procédure de mise à niveau après cette liste.

- Utilisation du DVD d'installation de Client Automation pour les ordinateurs Windows, Linux, MacIntel et UNIX.
- Utilisation du déploiement de l'infrastructure (DMDeploy) pour les ordinateurs agents Windows, Linux et MacIntel et du package "module(s) d'extension AM, RC, SD" (tous les modules d'extension de l'agent).

  Si tous les modules d'extension sont déjà installés sur les ordinateurs de l'agent, vous pouvez utiliser le package comprenant tous les modules d'extension de l'agent pour effectuer une mise à niveau. Si ce n'est pas le cas, vous pouvez quand même utiliser ce package mais sachez cependant que sous Windows, tous les modules d'extension qui ne sont pas encore installés seront ajoutés.
- Utilisation du déploiement de l'infrastructure pour les ordinateurs agents UNIX et du package "module(s) d'extension AM, SD" (tous les modules d'extension d'agent).
- Utilisation du déploiement de l'infrastructure pour les ordinateurs agents Windows, Linux, MacIntel et UNIX et des packages de modules d'extension d'un agent spécifique.
- Le déploiement de l'infrastructure vous permet de mettre à niveau un agent RC autonome.

- Utilisation de Software Delivery pour les agents Windows, Linux et MacIntel et du package "module(s) d'extension AM, RC, SD" (tous les modules d'extension de l'agent) ou des packages individuels de modules d'extension de l'agent.

  Si tous les modules d'extension sont déjà installés sur les ordinateurs de l'agent, vous pouvez utiliser le package comprenant tous les modules d'extension de l'agent pour effectuer une mise à niveau. Si ce n'est pas le cas, vous pouvez quand même utiliser ce package mais sachez cependant que sous Windows, tous les modules d'extension qui ne sont pas encore installés seront ajoutés.

- Utilisation de Software Delivery pour les ordinateurs agents UNIX et du package "module(s) d'extension AM, SD" (tous les modules d'extension d'agent) ou des packages de modules d'extension d'un agent spécifique.

  Remarque : Si vous effectuez la mise à niveau des agents DSM, vous devez appliquer les patchs suivants avant de procéder à la mise à niveau via Software Delivery.

  - AIX : RO01350
  - HP : RO01319
  - SUN : RO01315

Mise à niveau des agents à l'aide du DVD d'installation

Pour mettre à niveau les agents DSM à l'aide du DVD d'installation, insérez celui-ci dans l'ordinateur agent et suivez les étapes indiquées par l'assistant d'installation interactif.

Mise à niveau d'agents Windows à l'aide du déploiement d'infrastructure et du package "module(s) d'extension AM, RC, SD" (tous les modules d'extension de l'agent).

Si tous les modules d'extension sont déjà installés sur les ordinateurs agents, vous pouvez utiliser le package comprenant tous les modules d'extension de l'agent pour effectuer la mise à niveau. Cependant, le package comprenant tous les modules d'extension de l'agent met à niveau les modules d'extension AM, RC et SD, mais pas le module d'extension DTS. Utilisez le package DTS pour mettre à niveau le module d'extension DTS.

Remarque : Si vous utilisez le package comprenant tous les modules d'extension d'agent sous Windows, tous les modules d'extension qui ne sont pas déjà présents seront installés.

Pour mettre à niveau les agents DSM à l'aide du déploiement d'infrastructure pour les ordinateurs agents Windows et du package comprenant tous les modules d'extension, déployez le package "module(s) d'extension AM, RC, SD" sur les ordinateurs agents.

Pour que le programme d'installation lance la mise à niveau, vous devez spécifier les paramètres suivants dans le champ Options d'installation Windows supplémentaires de l'assistant de déploiement de l'infrastructure :

REINSTALL=ALL REINSTALLMODE=vomus

Mise à niveau d'agents Windows à l'aide du déploiement de l'infrastructure et du module d'extension individuel de l'agent

Pour mettre à niveau les agents DSM à l'aide du déploiement de l'infrastructure pour les ordinateurs agents Windows et des packages individuels de modules d'extension de l'agent, procédez comme suit :

- Déployez le package du module d'extension de l'agent Remote Control DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Remote Control est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

  Pour que le programme d'installation mette à niveau le module d'extension de l'agent, vous devez spécifier les paramètres suivants dans le champ Options d'installation Windows supplémentaires de l'assistant de déploiement de l'infrastructure :

  REINSTALL=ALL REINSTALLMODE=vomus

- Déployez le package du module d'extension de l'agent Software Delivery DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Software Delivery est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

  Pour que le programme d'installation mette à niveau le module d'extension de l'agent, vous devez spécifier les paramètres suivants dans le champ Options d'installation Windows supplémentaires de l'assistant de déploiement de l'infrastructure :

  REINSTALL=ALL REINSTALLMODE=vomus

- Déployez le package du module d'extension de l'agent Asset Management DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Asset Management est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

  Pour que le programme d'installation mette à niveau le module d'extension de l'agent, vous devez spécifier les paramètres suivants dans le champ Options d'installation Windows supplémentaires de l'assistant de déploiement de l'infrastructure :

  REINSTALL=ALL REINSTALLMODE=vomus

- Déployez le package du module d'extension de l'agent Inventaire de base DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Inventaire de base est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

  Pour que le programme d'installation mette à niveau le module d'extension de l'agent, vous devez spécifier les paramètres suivants dans le champ Options d'installation Windows supplémentaires de l'assistant de déploiement de l'infrastructure :

  REINSTALL=ALL REINSTALLMODE=vomus

Mise à niveau d'agents Linux ou MacIntel à l'aide du déploiement d'infrastructure et du package "module(s) d'extension AM, RC, SD" (tous les modules d'extension de l'agent).

Pour mettre à niveau les agents DSM à l'aide du déploiement d'infrastructure pour les ordinateurs agents Linux ou MacIntel et du package comprenant tous les modules d'extension, déployez le package "module(s) d'extension AM, RC, SD" sur les ordinateurs agents.

Par défaut, le package comprenant tous les modules d'extension de l'agent met à niveau les versions précédentes des modules d'extension de l'agent installés. Les nouveaux modules d'extension ne sont pas ajoutés.

Mise à niveau d'agents Linux ou MacIntel à l'aide du déploiement de l'infrastructure et du package individuel de modules d'extension de l'agent

Pour mettre à niveau les agents DSM à l'aide du déploiement de l'infrastructure pour les ordinateurs agents Linux ou MacIntel et des packages individuels de modules d'extension de l'agent, procédez comme suit :

- Déployez le package du module d'extension de l'agent Remote Control DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Remote Control est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

- Déployez le package du module d'extension de l'agent Software Delivery DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Software Delivery est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

- Déployez le package du module d'extension de l'agent Asset Management DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Asset Management est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

- Déployez le package du module d'extension de l'agent Inventaire de base DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Inventaire de base est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

Mise à niveau d'agents Linux ou MacIntel à l'aide de Software Delivery et du package "module(s) d'extension AM, RC, SD" (tous les modules d'extension de l'agent).

Pour mettre à niveau les agents DSM à l'aide de Software Delivery pour les ordinateurs agents Linux ou MacIntel et du package comprenant tous les modules d'extension de l'agent, procédez comme suit :

- Créez un job de déploiement Software Delivery avec le package comprenant tous les modules d'extension de l'agent.
- Planifiez le job Software Delivery pour être exécuté sur les ordinateurs équipés de l'agent.

  Par défaut, le package comprenant tous les modules d'extension de l'agent met à niveau les versions précédentes des modules d'extension de l'agent installés. Les nouveaux modules d'extension ne sont pas ajoutés.

Mise à niveau d'agents Linux ou MacIntel à l'aide de Software Delivery et du package individuel de modules d'extension de l'agent

Pour mettre à niveau les agents DSM à l'aide de Software Delivery pour les ordinateurs agents Linux ou MacIntel et des packages individuels de modules d'extension de l'agent, procédez comme suit :

- Créez un job de déploiement Software Delivery comportant au moins le package de modules d'extension Agent DSM + Agent Software Delivery.

  Si des versions antérieures d'autres modules d'extension de l'agent DSM ont également été installées sur l'ordinateur agent, incluez-les dans le job.
- Planifiez le job Software Delivery pour être exécuté sur les ordinateurs équipés de l'agent.

Mise à niveau d'agents Unix à l'aide du déploiement d'infrastructure et du package "module(s) d'extension AM, SD" (tous les modules d'extension d'agent)

Pour mettre à niveau les agents DSM à l'aide du déploiement d'infrastructure pour les ordinateurs agents Unix et du package comprenant tous les modules d'extension, déployez le package "module(s) d'extension AM, SD" sur les ordinateurs agents.

Par défaut, le package comprenant tous les modules d'extension de l'agent met à niveau les versions précédentes des modules d'extension de l'agent installés. Les nouveaux modules d'extension ne sont pas ajoutés.

Mise à niveau des agents Unix à l'aide du déploiement de l'infrastructure et des packages de modules d'extension d'un agent spécifique

Pour mettre à niveau les agents DSM à l'aide du déploiement de l'infrastructure pour les ordinateurs agents Unix et des packages de modules d'extension d'un agent spécifique, procédez comme suit :

- Déployez le package du module d'extension de l'agent Software Delivery DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Software Delivery est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

- Déployez le package du module d'extension de l'agent Asset Management DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Asset Management est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

- Déployez le package du module d'extension de l'agent Inventaire de base DSM vers l'ordinateur agent (si nécessaire).

  Si une version précédente du module d'extension de l'agent Inventaire de base est installée sur l'ordinateur agent, déployez la nouvelle version du module d'extension.

Mise à niveau d'agents Windows à l'aide de Software Delivery et du package "module(s) d'extension AM, RC, SD" (tous les modules d'extension de l'agent).

Si tous les modules d'extension sont déjà installés sur les ordinateurs équipés de l'agent, vous pouvez utiliser le package comprenant tous les modules d'extension de l'agent pour effectuer une mise à niveau. Si ce n'est pas le cas, vous pouvez quand même utiliser ce package mais sachez cependant que sous Windows, tous les modules d'extension qui ne sont pas encore installés seront ajoutés.

Pour mettre à niveau les agents DSM à l'aide de Software Delivery pour les ordinateurs agents Windows et du package comprenant tous les modules d'extension de l'agent, procédez comme suit :

- Créez un job de déploiement Software Delivery avec le package comprenant tous les modules d'extension de l'agent.
- Planifiez le job Software Delivery pour être exécuté sur les ordinateurs équipés de l'agent.

Mise à niveau des agents Windows à l'aide de Software Delivery et du package individuel de modules d'extension de l'agent

Pour mettre à niveau les agents DSM à l'aide de Software Delivery pour les ordinateurs agents Windows et des packages individuels de modules d'extension de l'agent, procédez comme suit :

- Créez un job de déploiement Software Delivery comportant au moins le package de modules d'extension Agent DSM + Agent Software Delivery.

  Si des versions antérieures d'autres modules d'extension de l'agent DSM ont également été installées sur l'ordinateur agent, incluez-les dans le job.
- Planifiez le job Software Delivery pour être exécuté sur les ordinateurs équipés de l'agent.

Mise à niveau d'agents Unix à l'aide de Software Delivery et du package "module(s) d'extension AM, SD" (tous les modules d'extension d'agent)

Remarque : Lorsque vous mettez à niveau des agents UNIX r11.1, appliquez les patchs suivants avant de procéder à la mise à niveau à l'aide de Software Delivery.

- AIX : RO01350
- HP : RO01319
- SUN : RO01315

Pour mettre à niveau les agents DSM à l'aide de Software Delivery sur les ordinateurs agents UNIX et du package comprenant tous les modules d'extension d'agent, procédez comme suit :

- Créez un job de déploiement Software Delivery avec le package comprenant tous les modules d'extension de l'agent.
- Planifiez le job Software Delivery pour être exécuté sur les ordinateurs équipés de l'agent.

  Par défaut, le package comprenant tous les modules d'extension de l'agent met à niveau les versions précédentes des modules d'extension de l'agent installés. Les nouveaux modules d'extension ne sont pas ajoutés.

Mise à niveau d'agents UNIX à l'aide de Software Delivery et du package de modules d'extension d'un agent spécifique

Remarque : Lorsque vous mettez à niveau des agents UNIX r11.1, appliquez les patchs suivants avant de procéder à la mise à niveau à l'aide de Software Delivery.

- AIX : RO01350
- HP : RO01319
- SUN : RO01315

Pour mettre à niveau les agents DSM à l'aide de Software Delivery pour les ordinateurs agents UNIX et des packages de modules d'extension d'un agent spécifique, procédez comme suit :

- Créez un job de déploiement Software Delivery comportant au moins le package de modules d'extension Agent DSM + Agent Software Delivery.

  Si des versions antérieures d'autres modules d'extension de l'agent DSM ont également été installées sur l'ordinateur agent, incluez-les dans le job.

- Planifiez le job Software Delivery pour être exécuté sur les ordinateurs équipés de l'agent.

Chapitre 7: Connecteur CA ITCM pour CA Catalyst

Les connecteurs CA Catalyst présentent les données de produit aux produits de consommation tels que CA Spectrum Service Assurance et CA IT Process Automation Manager pour la visualisation, l'analyse et la gestion dans un contexte unique et hétérogène.

Remarque : Vous pouvez installer le connecteur Client Automation avec un gestionnaire de domaines ou un serveur de modularité existant uniquement sur les systèmes d'exploitation Windows.

Le connecteur Client Automation prend en charge SSA 3.2.0. Il se connecte au gestionnaire de domaines DSM ou à un serveur de modularité autonome enregistré sur un gestionnaire de domaines pour mettre à disposition les données de Client Automation utilisées par les produits qui exploitent l'infrastructure de CA Catalyst. L'intégration des données Client Automation à des produits consommateurs, comme CA Spectrum SA, permet le rapprochement et la corrélation des propriétés d'entité avec des éléments de configuration existants. Elle vous permet également d'évaluer les données dans un contexte de service métier différent et plus général.

Remarque : Le connecteur CA ITCM 3.2.0 prend en charge uniquement Northbound sur SOI 3.2.0.

L'intégration du connecteur CA Catalyst suppose un connecteur Client Automation par domaine. Le connecteur de Client Automation se connecte avec le gestionnaire de domaines à l'aide de la fonctionnalité ou des composants Client Automation suivants :

- Services Web de Client Automation

  Les services Web de Client Automation sont utilisés pour récupérer des informations sur les éléments de configuration à publier dans le connecteur CA Catalyst.

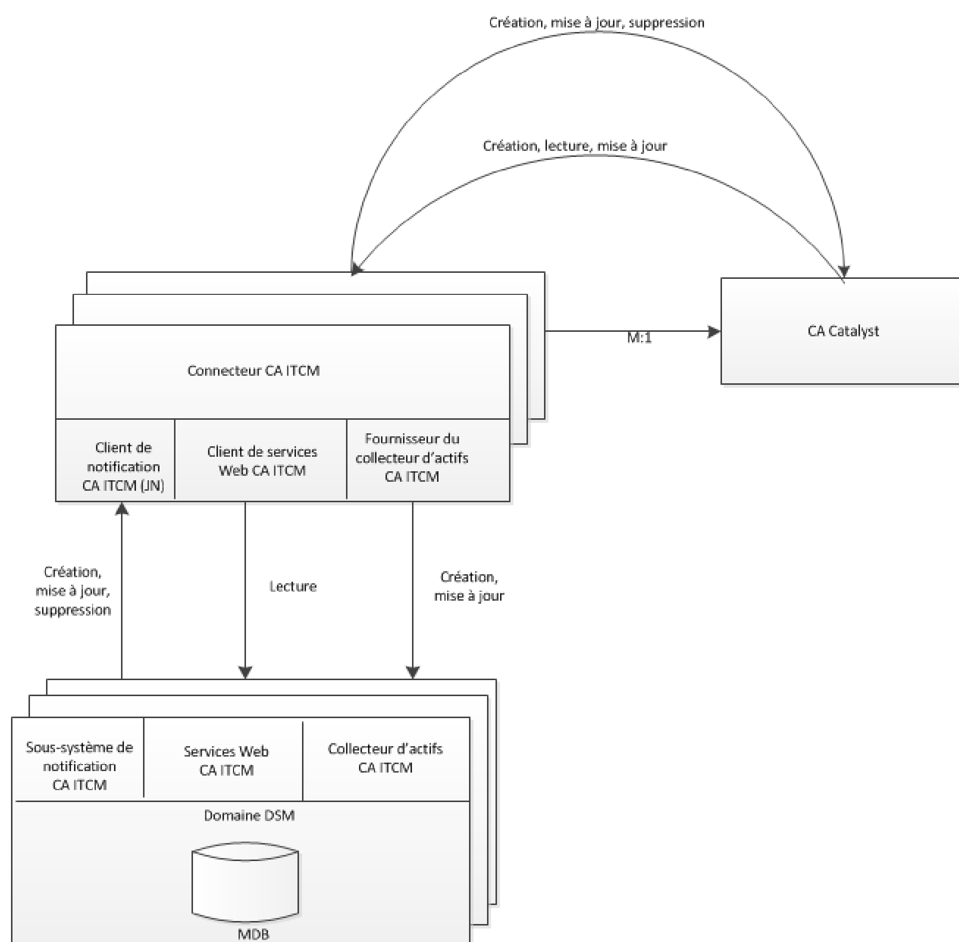
- Sous-système de notifications d’événements de Client Automation

  Les événements concernant les mises à jour des éléments de configuration publiés sont reçus dans le sous-système de notification d'événements de Client Automation.

- Collecteur d'actifs

  Le collecteur d'actifs est utilisé durant les opérations d'abonnement à CA Spectrum SA pour les données d'élément de configuration d'ordinateur. Les fichiers du collecteur d'actifs permettent de déplacer les données de création et les données de mise à jour entrantes du connecteur vers la MDB Client Automation.

Le graphique suivant résume l'intégration entre Client Automation et le connecteur CA Catalyst :



Remarque : Pour plus d'informations générales sur l'infrastructure de CA Catalyst et ses connecteurs, sur tous les connecteurs et sur les intégrations de connecteurs personnalisés, consultez le *Manuel du connecteur* distribué avec CA Spectrum SA. Pour des informations complètes sur l'installation, la configuration et l'utilisation du connecteur Client Automation, consultez le *Manuel du connecteur de CA IT Client Manager* distribué également avec CA Spectrum SA.

Chapitre 8: Virtualisation de l'ordinateur de bureau

Cette section inclut les scénarios sur l'utilisation de la fonctionnalité de prise en charge de la virtualisation d'ordinateur de bureau. Client Automation vous permet de gérer votre infrastructure d'ordinateurs de bureau virtuels sur VMware View et Citrix XenDesktop. CA ITCM vous permet d'effectuer les tâches suivantes :

- Gérer le modèle Or, les vDisk et les ordinateurs de bureau virtuels à partir de l'explorateur DSM.
- Configurer la réinstallation automatique de logiciels installés sur des ordinateurs de bureau virtuels, sans affecter les modifications apportées après un redémarrage ou une mise à jour des ordinateurs de bureau avec une nouvelle version du modèle Or.

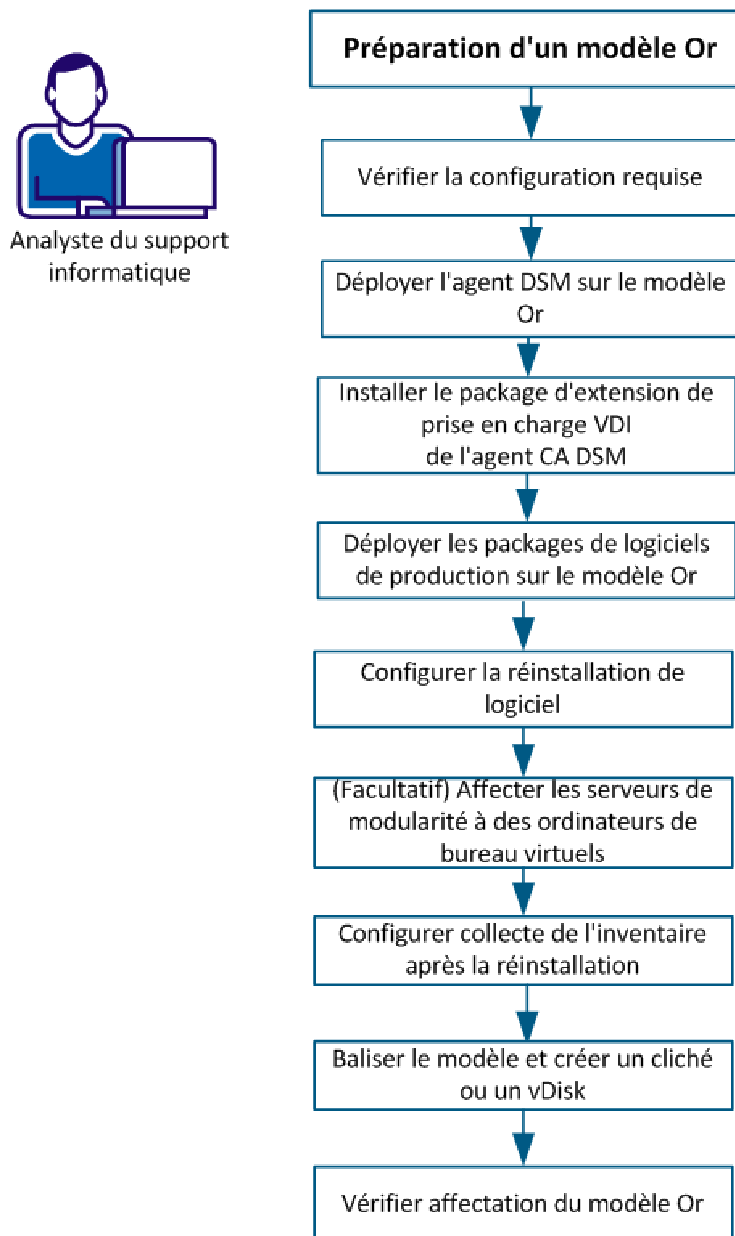
  Par exemple, les logiciels installés sur un ordinateur de bureau virtuel basé sur vDisk en mode standard sont perdus après la déconnexion. Vous pouvez configurer CA ITCM pour réinstaller automatiquement ces logiciels à la connexion suivante.
- CA ITCM inclut une nouvelle identification d'ordinateur de bureau virtuel, un nouveau schéma d'enregistrement, une vitesse d'enregistrement d'actif améliorée, ainsi que de nouveaux rapports et requêtes.

  Remarque : La gestion des profils d'utilisateur, des données de l'utilisateur, des personnalités d'utilisateur ou la configuration des ordinateurs de bureau n'est pas prise en charge dans cette version. Les méthodes Microsoft, telles que les profils d'utilisateurs itinérants et la redirection de dossier, permettent de gérer ces tâches. Pour plus d'informations, reportez-vous à la documentation Microsoft.

Préparation d'un modèle Or

En tant qu'analyste du support informatique, vous devez préparer le modèle Or afin d'intégrer votre solution de bureau virtuel à Client Automation. Cette intégration vous aide à gérer le modèle Or, les clones VMware View, les bureaux virtuels Citrix PVS ou les bureaux virtuels MCS à partir de Client Automation.

Le diagramme suivant illustre les étapes pour préparer un modèle Or :



La préparation d'un modèle Or implique l'exécution des tâches suivantes :

1. Vérification de la configuration requise (page 297)
2. Déploiement de l'agent DSM sur le modèle Or (page 298)
3. Installation du package d'extension de prise en charge VDI de l'agent CA DSM (page 299)
4. Déploiement des packages de logiciels de production sur le modèle Or (page 299)
5. Configuration de la réinstallation de logiciel (page 300)
6. Balisage du modèle et création d'un cliché ou d'un vDisk (page 313)
7. (Facultatif) Affectation de serveurs de modularité à des ordinateurs de bureau virtuels (page 311)
8. Configuration de la collecte de l'inventaire pour la réinstallation de logiciel (page 313)
9. Vérification de l'affectation du modèle Or (page 314)

Vérification de la configuration requise

Pour préparer un modèle Or, vérifiez que la configuration requise suivant est respectée :

- Vérifiez que l'agent de bureau virtuel est installé sur l'ordinateur du modèle Or.

  Remarque : L'implémentation de l'intégration à Client Automation requiert une bonne maîtrise pratique des solutions de bureau virtuel telles que VMware View et Citrix XenDesktop.

- Vérifiez que le périphérique cible Citrix PVS est installé sur l'ordinateur modèle Or si vous voulez créer des ordinateurs de bureau virtuels Citrix utilisant un vDisk.
- (Citrix XenDesktop 7 uniquement) Vérifiez que .Net 3.5 est disponible.

Déploiement de l'agent DSM sur le modèle Or

Client Automation fournit différents packages d'agent DSM selon les fonctionnalités dont vous avez besoin. Au minimum, vous avez besoin de l'agent commun DSM et de l'agent Software Delivery (module d'extension de Software Delivery et de l'agent CA DSM). Si vous voulez toutes les fonctionnalités, déployez le package des modules d'extension de l'agent CA DSM, d'AM, de RC et de SD.

Remarque : L'agent DSM fait référence à l'agent commun DSM et l'agent Software Delivery (module d'extension de Software Delivery et de l'agent CA DSM), et non à l'agent complet comme susmentionné.

Grâce au déploiement de l'agent DSM sur le modèle Or, l'agent DSM est disponible sur les ordinateurs de bureau virtuels créés à partir du modèle Or. Le modèle Or et tous les ordinateurs de bureau virtuels sont ajoutés en tant qu'ordinateurs gérés dans Client Automation.

Procédez comme suit:

1. A partir de l'explorateur DSM, accédez au Panneau de configuration, puis cliquez sur Déploiement, Assistant de déploiement de l'infrastructure.
2. Suivez les instructions dans l'assistant et effectuez les tâches suivantes :
   - Sélectionnez un package d'agent selon les fonctionnalités dont vous avez besoin.
   - Sélectionnez le modèle Or comme ordinateur cible dans l'assistant.
   - Entrez l'adresse IP ou le nom de domaine complet (FQDN) du serveur de modularité auprès duquel l'agent déployé est enregistré.
3. Cliquez sur Terminer.

   Un job de déploiement est créé sous Panneau de configuration, Déploiement, Etat du job de déploiement. Le job est transmis au modèle Or.
4. Surveillez l'état du job sous Panneau de configuration, Déploiement, Etat du job de déploiement.

   Une fois le déploiement effectué, l'agent est automatiquement enregistré auprès du serveur de modularité. Après l'enregistrement, le modèle Or s'affiche dans le gestionnaire de domaines.

Remarque : Par défaut, le modèle Or et les ordinateurs de bureau virtuels provisionnés à partir de celui-ci rendent compte au même serveur de modularité. Vous pouvez affecter un serveur de modularité différent à une plage d'ordinateurs de bureau virtuels en fonction du modèle d'attribution de nom de ces derniers. Reportez-vous à la rubrique (Facultatif) Affectation de serveurs de modularité à des ordinateurs de bureau virtuels (page 311).

Installation du package d'extension de prise en charge VDI de l'agent CA DSM

Installez le package d'extension de prise en charge VDI de l'agent CA DSM sur le modèle Or pour permettre la réinstallation de logiciel et l'intégration entre Client Automation et VMware View ou Citrix XenDesktop. L'extension permet à l'agent DSM de faire fonctionner et de gérer l'environnement de bureau virtuel.

Le package d'extension de prise en charge VDI de l'agent CA DSM effectue les tâches suivantes :

- Il active l'utilisation de la base de données des états de logiciel et, si nécessaire, définit les chemins d'accès.
- Il définit l'agent sur le mode de modèle Or.
- Il copie sur le modèle Or un ensemble de scripts de clonage qui seront utilisés pendant la réinstallation de logiciel.

Procédez comme suit:

1. Cliquez avec le bouton droit de la souris sur le modèle Or dans l'explorateur DSM et sélectionnez Jobs logiciels, Déployer le package logiciel.

   L'assistant de déploiement de packages logiciels s'ouvre.

2. Suivez les instructions de l'assistant. Spécifiez les tâches suivantes dans l'assistant :

   - Sélectionnez le package d'extension de prise en charge VDI de l'agent CA DSM pour Windows FRA sous Packages logiciels DSM.

     Remarque : Le package fournit une solution commune pour VMWare View et Citrix XenDesktop, et prend également en charge les paramètres Sysprep sous VMware View.

   - Planifiez l'heure et entrez le nom du conteneur de jobs.

3. Cliquez sur Terminer.

   La boîte de dialogue Configurer des jobs s'ouvre.

4. Cliquez sur OK.

   Le package est livré à l'heure planifiée.

5. Pour surveiller l'état du de job, dans l'explorateur DSM, sélectionnez le modèle Or, Jobs, Jobs logiciels.

Déploiement des packages de logiciels de production sur le modèle Or

Vous pouvez utiliser Software Delivery pour déployer des packages de logiciels de production sur le modèle Or. Les applications logicielles qui sont installées sur le modèle Or sont automatiquement disponibles sur les ordinateurs de bureau virtuels créés à partir du modèle Or.

Procédez comme suit:

1. Cliquez avec le bouton droit de la souris sur le modèle Or dans l'explorateur DSM et sélectionnez Jobs logiciels, Déployer le package logiciel.

   L'assistant de déploiement de packages logiciels s'ouvre.

2. Suivez les instructions de l'assistant. Spécifiez les actions suivantes dans l'assistant :

   - Sélectionnez les packages logiciels et les procédures à déployer.
   - Entrez le nom du conteneur de jobs

3. Ouvrez la boîte de dialogue des paramètres de job avancés et cliquez sur Terminer.

   La boîte de dialogue Configurer des jobs s'ouvre.

4. Cliquez sur Jobs, Options de job, Stocker les packages dans la bibliothèque intermédiaire du serveur de modularité.

5. Cliquez sur OK.

   Les packages spécifiés sont stockés sur le serveur de modularité du modèle Or. Le package est livré à l'heure planifiée.

Configuration de la réinstallation de logiciel

Les logiciels qui sont installés sur des ordinateurs de bureau virtuels non persistants sont perdus après un redémarrage, une fermeture de session ou une mise à jour de l'ordinateur vers une version plus récente du modèle Or. Vous pouvez configurer Client Automation pour réinstaller les logiciels dans ces cas. Client Automation utilise une base de données des états de logiciel d'instance qui contient les informations de tous les jobs logiciels que l'agent exécute sur les ordinateurs de bureau virtuels. Les ordinateurs de bureau virtuels incluent les détails de la base de données des états de logiciel d'instance et du contexte d'exécution. Ces informations sont importantes lors de la réinstallation de logiciel par Client Automation.

Selon la solution de virtualisation de bureau et les paramètres de pool/groupe d'ordinateurs de bureau, vous configurez la réinstallation de logiciel de façons différentes :

Vue VMware

- Pour des groupes d'ordinateurs de bureau avec la personnalisation *quickprep,* effectuez une des tâches de configuration suivantes :
  - Configuration des paramètres de réinstallation de logiciel dans la stratégie de configuration (page 305)
  - Configuration des paramètres de pool pour exécuter le fichier Compose.bat sur les ordinateurs de bureau virtuels (page 302)

  Remarque : Si vous configurez à la fois la stratégie et les paramètres de pool, ces derniers sont prioritaires.
- Pour les groupes d'ordinateurs de bureau avec la personnalisation *Sysprep*, effectuez la tâche de configuration suivante :
  - Configuration des paramètres de réinstallation de logiciel dans la stratégie de configuration (page 305)

Citrix XenDesktop

- Pour des ordinateurs de bureau créés à partir de MCS, effectuez la tâche de configuration suivante :
  - Configuration des paramètres de réinstallation de logiciel dans la stratégie de configuration (page 305)
- Pour les ordinateurs de bureau utilisant un vDisk, effectuez une des tâches de configuration suivantes :
  - Configuration des paramètres de réinstallation de logiciel dans la stratégie de configuration (page 305)
  - Configuration des données de personnalité sur les unités cibles (page 308)

  Remarque : Si vous configurez à la fois la stratégie et les données de personnalité, ces dernières sont prioritaires.

Remarque : Vous pouvez également modifier d'autres stratégies de configuration. Pour plus d'informations sur ces stratégies, reportez-vous à la rubrique Stratégies de configuration pour la prise en charge de la virtualisation des ordinateurs de bureau (page 314).

Configuration des paramètres de pool pour exécuter le fichier Compose.bat sur les ordinateurs de bureau virtuels

Lorsque vous créez le pool, sous Personnalisations d'invité, spécifiez la commande suivante dans le script de post-synchronisation :

```
Compose.bat [ISDBPath=<Path>] [Run=<Run>] [ISDBUser=<User>
ISDBPassword=<Password>]
```

ISDBPATH

Spécifie le chemin d'accès à l'emplacement de stockage de la base de données de logiciel d'instance. Le chemin d'accès peut être local ou réseau selon le type de pool. Spécifiez un chemin réseau pour les pools non persistants et un chemin local ou réseau pour les pools persistants. Les variables d'environnement et les macros prédéfinies comme {SCALABILITY_SERVER} et {POOL_NAME} sont permises dans le chemin d'accès.

Exemple : \\{SCALABILITY_SERVER}\%COMPUTERNAME%

Important : Sous Windows 7, si le paramètre de chemin d'accès contient la variable d'environnement %USERNAME%, ne transférez pas ce paramètre comme paramètre de ligne de commande au fichier Compose.bat. Incluez plutôt tous les paramètres dans le fichier Compose.bat (pour VMware View uniquement).

{SCALABILITY_SERVER}

Renvoie le serveur de modularité auquel l'ordinateur de bureau virtuel rend compte. Par défaut, les ordinateurs de bureau virtuels rendent compte au même serveur de modularité que le modèle Or. Si vous avez changé l'affectation de serveur de modularité explicitement (page 311), la macro renvoie le nouveau nom de serveur de modularité.

{POOL_NAME}

Renvoie le nom de pool de l'ordinateur de bureau virtuel. Cette macro s'applique uniquement à VMware View.

Utilisation persistante

Vous pouvez utiliser des variables d'environnement, telles que %COMPUTERNAME% dans le chemin d'accès ISDB.

Exemple : \\MachineName\{POOL_NAME}\%COMPUTERNAME%

Cette option permet d'obtenir un chemin d'accès unique pour un utilisateur, car un ordinateur de bureau virtuel persistant est toujours affecté au même utilisateur.

Utilisation non persistante

Vous pouvez inclure les variables d'environnement propres à un utilisateur %USERNAME% et %USERDOMAIN% de manière à identifier de façon univoque la base de données des états de logiciel pour un utilisateur.

Exemple : \\MachineName\{POOL_NAME}\%USERNAME%

Remarque : Si vous utilisez des chemins d'accès de partage réseau, faites attention de bien sélectionner l'emplacement lorsque plusieurs pools d'ordinateurs de bureau sont affectés à un utilisateur unique. Assurez-vous de ce que l'état de logiciel de l'ordinateur de bureau virtuel utilisé par un utilisateur dans un pool ne soit pas écrasé par les données d'un autre ordinateur de bureau virtuel utilisé par le même utilisateur dans un autre pool. Par exemple, Utilisateur1 a accès aux pools non persistants poolA et poolB. Si le chemin d'accès aux pools est spécifié sous la forme //<nom_ordinateur>/<nom_partage>/Database/%USERNAME%, vous pouvez écraser l'état de logiciel de Utilisateur1, si celui-ci se connecte et utilise les deux ordinateurs de bureau virtuels dans les deux pools. Par conséquent, veillez à définir des chemins d'accès différents, comme suit :

- “/<nom_ordinateur>/<nom_partage>/PoolA/%USERNAME%”
- “/<nom_ordinateur>/<nom_partage>/PoolB/%USERNAME%”

ISDBUSER

Spécifie le nom d'utilisateur pour se connecter au chemin d'accès à la base de données de logiciel d'instance dans un partage réseau. Le nom d'utilisateur doit être chiffré à l'aide de la commande sd_acmd encrypt.

ISDBPASSWORD

Spécifie le mot de passe pour se connecter au chemin d'accès à la base de données de logiciel d'instance dans un partage réseau. Le mot de passe doit être chiffré à l'aide de la commande sd_acmd encrypt.

RUN

Indique quand le processus de réinstallation hors ligne après un arrêt brutal doit être exécuté. Les valeurs valides sont OnRecompose et OnLogon.

OnRecompose

Indique que la réinstallation hors ligne après un arrêt brutal est initialisée lorsque l'ordinateur de bureau démarre après une actualisation ou une recomposition. Utilisez cette option pour des groupes d'ordinateurs de bureau où l'affectation d'ordinateur de bureau à des utilisateurs est fixe, comme des clones liés persistants.

OnLogon

Spécifie que le processus de réinstallation hors ligne après un arrêt brutal est initié lorsque l'utilisateur se connecte.

Utilisez cette option pour des groupes d'ordinateurs de bureau où l'affectation d'ordinateur de bureau aux utilisateurs varie d'une session à l'autre, comme les ordinateurs de bureau non persistants.

Exemples :

- **Utilisation persistante :** Compose.bat "ISDBPath=<chemin_accès>" "Run=OnRecompose"
- **Utilisation non persistante :** Compose.bat "ISDBPath=<chemin_accès>" "Run=OnLogon"

Configuration des paramètres de réinstallation de logiciel dans la stratégie de configuration

Procédez comme suit:

1. Accédez au Panneau de configuration, puis cliquez sur Stratégie de configuration, Stratégie par défaut de l'ordinateur, DSM, Software Delivery, Agent.
2. Sélectionnez RAC : paramètres de réinstallation de logiciel pour un ordinateur virtuel pour afficher les attributs suivants :

   Modèle de nommage de l'agent

   Spécifie le modèle de nommage de l'agent de l'ordinateur de bureau virtuel. Pour VMware View, le modèle de nommage doit correspondre au modèle de nommage défini dans le pool VMware. Pour XenDesktop, le modèle de nommage doit être *nom##*. Vous ne pouvez spécifier cet espace réservé (#) ni au début ni plus d'une fois.

   De

   Spécifie le début de la plage d'ordinateurs de bureau à inclure. La plage peut être un nombre ; XenDesktop permet toutefois aussi de spécifier des caractères alphabétiques. *De* spécifie le début du modèle de nommage. Le début et la longueur de l'espace réservé doivent être égaux, et la valeur *A* peut être supérieure à la longueur de l'espace réservé.

   A

   Spécifie la fin de la plage d'ordinateurs de bureau à inclure. La plage peut être un nombre ; XenDesktop permet toutefois aussi de spécifier des caractères alphabétiques.

Exemples : Modèle de nommage d'agent pour VMware View

Modèle de nommage de l'agent	De	A	Noms d'ordinateur de bureau possibles
Name-{n}	1	100	Name-1, Name-2....Name-100

Exemples : Modèle de nommage d'agent pour Citrix XenDesktop

Modèle de nommage de l'agent	De	A	Noms d'ordinateur de bureau possibles
Name#	1	100	Name1, Name2, ...Name100
Name###	1	100	Name001, Name002.....Name100
Name##	AA	AZ	NameAC, NameAE,...NameAZ

Chemin d'accès à la base de données de logiciel d'instance

Spécifie le chemin d'accès à l'emplacement de stockage de la base de données de logiciel d'instance. Le chemin d'accès peut être local ou réseau selon le type de pool. Spécifiez un chemin réseau pour les pools non persistants et un chemin local ou réseau pour les pools persistants (clones liés persistants pour VMware View et groupes d'ordinateurs de bureau utilisant un vDisk en mode différentiel pour Citrix XenDesktop avec l'affectation d'ordinateur de bureau fixe). Dans ce dernier cas, la spécification d'un chemin d'accès local est uniquement possible si le disque persistant associé à l'ordinateur de bureau virtuel est disponible. Les variables d'environnement et les macros prédéfinies comme {SCALABILITY_SERVER}, {GROUP_NAME} et {POOL_NAME} sont permises comme parties du chemin d'accès.

Exemple : \\{SCALABILITY_SERVER}\{GROUP_NAME}\%COMPUTERNAME%

{GROUP_NAME}

Renvoie le nom du groupe d'ordinateurs de bureau auquel appartient l'ordinateur de bureau virtuel. Cette macro s'applique uniquement à Citrix XenDesktop.

{POOL_NAME}

Renvoie le nom de pool de l'ordinateur de bureau virtuel. Cette macro s'applique uniquement à VMware View.

{SCALABILITY_SERVER}

Renvoie le serveur de modularité auquel l'ordinateur de bureau virtuel rend compte. Par défaut, les ordinateurs de bureau virtuels rendent compte au même serveur de modularité que le modèle Or ou le vDisk. Si vous avez changé l'affectation de serveur de modularité explicitement (page 311), la macro renvoie le nouveau nom de serveur de modularité.

Remarque : Pour XenDesktop, vous pouvez affecter plusieurs utilisateurs à un ordinateur de bureau unique dans un groupe statique en pool. Pour prendre en charge la réinstallation de logiciels installés par l'utilisateur dans ce cas, spécifiez le chemin d'accès à la base de données de logiciel d'instance de la façon suivante : *<nom_serveur>\%computername%\%username%.* Définissez également le contexte d'exécution sur *OnLogon.*

Nom d'utilisateur

Spécifie le nom d'utilisateur pour se connecter au chemin d'accès à la base de données de logiciel d'instance dans un partage réseau. Le nom d'utilisateur est chiffré à l'aide de la commande sd_acmd encrypt.

Mot de passe

Spécifie le mot de passe pour se connecter au chemin d'accès à la base de données de logiciel d'instance dans un partage réseau. Le mot de passe est chiffré à l'aide de la commande sd_acmd encrypt.

Exécuter

Indique quand le processus de réinstallation hors ligne après un arrêt brutal doit être exécuté. Les valeurs permises sont OnRecompose et OnLogon.

OnRecompose

Indique que le processus de réinstallation hors ligne après un arrêt brutal doit être initié lorsque l'ordinateur de bureau démarre après une opération d'actualisation ou de recomposition (dans le cas de VMware View), lorsque l'ordinateur de bureau est réinitialisé ou qu'un cliché est mis à jour (dans le cas de Citrix MCS) et lorsque le vDisk est mis à jour ou que l'ordinateur de bureau est réinitialisé (dans le cas d'ordinateurs de bureau virtuels diffusés en continu)..

Utilisez cette option pour des groupes d'ordinateurs de bureau où l'affectation d'ordinateur de bureau à des utilisateurs est fixe, comme des clones liés persistants, des ordinateurs de bureau statiques en pool et des ordinateurs de bureau utilisant des vDisks en mode différentiel.

OnLogon

Spécifie que le processus de réinstallation hors ligne après un arrêt brutal est initié lorsque l'utilisateur se connecte.

Utilisez cette option pour des groupes d'ordinateurs de bureau en pool où l'affectation d'ordinateur de bureau aux utilisateurs varie d'une session à l'autre, comme les ordinateurs de bureau non persistants, les ordinateurs de bureau aléatoires en pool et les ordinateurs de bureau en pool utilisant des vDisks en mode standard.

3. Enregistrez et scellez la stratégie.

   La configuration de réinstallation de logiciel est appliquée sur le modèle Or.

Configuration des données de personnalité sur les unités cibles

Pour Citrix XenDesktop, configurez les données de personnalité après avoir créé les catalogues à l'aide de l'assistant d'installation de XenDesktop ou de l'assistant d'installation de machine virtuelle diffusée en continu et avant de créer le ou les groupes d'ordinateurs de bureau à partir des ordinateurs.

Procédez comme suit:

1. Ouvrez la boîte de dialogue Target Device Properties dans la console des services de provisionnement Citrix pour un ordinateur de bureau virtuel.
2. Cliquez sur l'onglet Personality et ajoutez les paramètres suivants :

CA_DSM_ISDBPATH

Spécifie le chemin d'accès à l'emplacement de stockage de la base de données de logiciel d'instance. Le chemin d'accès peut être local ou réseau selon le type de pool. Spécifiez un chemin réseau pour les pools non persistants et un chemin local ou réseau pour les pools persistants (groupes d'ordinateurs de bureau utilisant un vDisk en mode différentiel pour Citrix XenDesktop avec l'affectation d'ordinateur de bureau fixe).

Dans ce dernier cas, la spécification d'un chemin d'accès local est uniquement possible si le disque persistant associé à l'ordinateur de bureau virtuel est disponible. Les variables d'environnement et les macros prédéfinies comme {SCALABILITY_SERVER} et {GROUP_NAME} sont permises dans le chemin d'accès.

Exemple : \\{SCALABILITY_SERVER}\{GROUP_NAME}\%COMPUTERNAME%

{GROUP_NAME}

Renvoie le nom du groupe d'ordinateurs de bureau auquel appartient l'ordinateur de bureau virtuel. Cette macro s'applique uniquement à Citrix XenDesktop.

{SCALABILITY_SERVER}

Renvoie le serveur de modularité auquel l'ordinateur de bureau virtuel rend compte. Par défaut, les ordinateurs de bureau virtuels rendent compte au même serveur de modularité que le modèle Or ou le vDisk. Si vous avez changé l'affectation de serveur de modularité explicitement (page 311), la macro renvoie le nouveau nom de serveur de modularité.

CA_DSM_ISDBUSER

Spécifie le nom de l'utilisateur de la base de données de logiciel d'instance dans un formulaire chiffré. Le nom d'utilisateur est chiffré à l'aide de la commande sd_acmd encrypt.

CA_DSM_ISDBPASSWORD

Spécifie le mot de passe de la base de données de logiciel d'instance chiffré dans un formulaire chiffré. Le mot de passe est chiffré à l'aide de la commande sd_acmd encrypt.

CA_DSM_RUN

Indique quand le processus de réinstallation hors ligne après un arrêt brutal doit être exécuté. Les valeurs valides sont OnRecompose et OnLogon.

OnRecompose

Indique que le processus de réinstallation hors ligne après un arrêt brutal doit être initié lorsque l'ordinateur de bureau démarre après une réinitialisation ou une mise à jour de cliché (dans le cas de Citrix MCS) et lorsque le vDisk est mis à jour ou réinitialisé (dans le cas d'ordinateurs de bureau virtuels diffusés en continu).

Utilisez cette option pour des groupes d'ordinateurs de bureau où l'affectation d'ordinateur de bureau à des utilisateurs est fixe, comme des ordinateurs de bureau statiques en pool et des ordinateurs de bureau utilisant des vDisks en mode différentiel.

OnLogon

Spécifie que le processus de réinstallation hors ligne après un arrêt brutal est initié lorsque l'utilisateur se connecte.

Utilisez cette option pour des groupes d'ordinateurs de bureau en pool où l'affectation d'ordinateur de bureau aux utilisateurs varie d'une session à l'autre, comme les ordinateurs de bureau aléatoires en pool et les ordinateurs de bureau en pool utilisant des vDisks en mode standard.

3. Enregistrez les propriétés.

   L'ordinateur de bureau virtuel est configuré pour inclure les détails de la base de données des états de logiciel d'instance.

4. Effectuez l'une des tâches suivantes :

   ■ Effectuez les étapes 1 à 3 sur tous les ordinateurs de bureau virtuels.

   ■ Copiez les paramètres d'un ordinateur de bureau sur tous les ordinateurs de bureau virtuels.

Vous avez maintenant configuré des données de personnalité sur les unités cibles.

Diffusion en continu de données de personnalité vers les ordinateurs de bureau virtuels dans XenDesktop 5.5

Avec l'agent de bureau virtuel Citrix XenDesktop 5.5, les données de personnalité des ordinateurs de bureau virtuels ne sont pas diffusées en continu vers les ordinateurs de bureau virtuels au démarrage.

Lorsque la configuration de la base de données de logiciel d'instance est réalisée à l'aide de données de personnalité et non de la stratégie de configuration, la fonctionnalité de réinstallation de logiciel est affectée.

Utilisez les correctifs suivants de l'agent de bureau virtuel Citrix pour éviter ce problème.

- http://support.citrix.com/article/CTX131268 (version 32 bits)
- http://support.citrix.com/article/CTX131269 (version 64 bits)

Types d'ordinateur de bureau virtuels pris en charge pour la réinstallation de logiciel

Client Automation prend en charge la réinstallation de logiciel sur les types d'ordinateur de bureau virtuel suivants :

VMware View :

- Clones liés

Citrix XenDesktop :

- Ordinateurs de bureau statiques en pool
- Ordinateurs de bureau aléatoires en pool
- Ordinateurs de bureau diffusés en continu
- Ordinateurs de bureau existants basés sur le catalogue et utilisant un vDisk en mode standard ou différentiel

Remarque : Vous pouvez créer les types suivants à partir du modèle Or, mais aucun support n'est requis pour la réinstallation de logiciel. Seuls les enregistrements de logiciel de modèle sont signalés au gestionnaire de domaines au démarrage. Vous pouvez gérer les types suivants indépendamment comme des agents Client Automation standard.

- Ordinateurs de bureau utilisant un vDisk en mode privé
- Ordinateurs de bureau dédiés (via MCS)

Important : Vérifiez que les ordinateurs de bureau virtuels sont configurés pour redémarrer lorsque l'utilisateur se déconnecte pour lancer des clones liés flottants dans VMware View. Lorsque vous créez des groupes statiques en pool avec un ordinateur de bureau affecté à plusieurs utilisateurs, spécifiez ce paramètre manuellement afin que la réinstallation de logiciel fonctionne comme prévu.

(Facultatif) Affectation de serveurs de modularité à des ordinateurs de bureau virtuels

Tous les ordinateurs de bureau virtuels rendent compte au même serveur de modularité que l'agent du modèle Or ou du vDisk. Vous pouvez affecter des serveurs de modularité différents aux agents des ordinateurs de bureau virtuels pour distribuer la charge sur le serveur. Avant de poursuivre, vous devez décider du modèle de nommage que vous voulez utiliser pour les ordinateurs de bureau créés à partir du modèle Or. En fonction des modèles de nommage des ordinateurs de bureau, vous pouvez affecter des serveurs de modularité différents aux agents de ces ordinateurs. Vous pouvez également configurer le nombre d'ordinateurs de bureau que vous voulez affecter au serveur.

Procédez comme suit:

1. Dans l'explorateur DSM, ouvrez la stratégie de configuration que vous voulez appliquer sur le modèle Or.
2. Sélectionnez DSM, Composants communs, Enregistrement.
3. Double-cliquez sur la stratégie de configuration des serveurs de modularité.

4. Cliquez sur Ajouter une ligne et spécifiez le modèle de nommage et la plage dans les champs suivants :

Modèle de nommage de l'agent

Spécifie le modèle de nommage de l'agent de l'ordinateur de bureau virtuel. Pour VMware View, le modèle de nommage doit être name-{n} et pour XenDesktop, name##. Vous pouvez aussi opter pour un modèle de nommage différent.

Serveur de modularité.

Spécifie le serveur de modularité que vous voulez affecter au modèle et à la plage spécifiés.

De

Spécifie le début de la plage d'ordinateurs de bureau à inclure. La plage peut être un nombre ; Citrix XenDesktop permet toutefois aussi de spécifier des caractères alphabétiques. Le début et la longueur de l'espace réservé doivent être égaux, et la valeur *A* peut être supérieure à la longueur de l'espace réservé.

A

Spécifie la fin de la plage d'ordinateurs de bureau à inclure. La plage peut être un nombre ; Citrix XenDesktop permet toutefois aussi de spécifier des caractères alphabétiques.

Exemples : Modèle de nommage d'agent pour Citrix XenDesktop

Modèle de nommage de l'agent	De	A	Noms d'ordinateur de bureau possibles
Name#	1	100	Name1, Name2, Name100
Name###	1	100	Name001, Name002, Name100
Name##	AB	BC	NameAC, NameAE, NameAZ

Exemples : Modèle de nommage d'agent pour VMware View

Modèle de nommage de l'agent	De	A	Noms d'ordinateur de bureau possibles
Name-{n}	1	100	Name-1, Name-2, Name-100

5. Enregistrez et scellez la stratégie.

Lorsque les ordinateurs de bureau virtuels sont créés, ils sont automatiquement affectés à un serveur de modularité en fonction de la configuration que vous avez spécifiée.

Configuration de la collecte de l'inventaire pour la réinstallation de logiciel

Configurez la collecte de l'inventaire pour dresser l'inventaire à partir de l'ordinateur de bureau virtuel, soit immédiatement à la suite de la réinstallation après un arrêt brutal (RAC), soit lorsque l'utilisateur se connecte après cette réinstallation. La collecte de l'inventaire vous aide à vérifier si toutes les applications logicielles sont réinstallées.

Procédez comme suit:

1. Accédez au Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Stratégie par défaut de l'ordinateur, DSM, Software Delivery, Agent.
2. Sélectionnez la stratégie de configuration RAC : collecte d'inventaire après la réinstallation et définissez la valeur sur un des attributs suivants :

   No

   Spécifie que l'inventaire n'est pas collecté après la réinstallation, mais pendant l'exécution normale de l'agent AM qui peut s'exécuter avant ou après la RAC.

   Immédiatement

   Spécifie que l'inventaire est collecté immédiatement après la réinstallation de logiciel. Le système signale les logiciels réinstallés dans le cadre de l'inventaire des logiciels et les informations d'unité clientes comme l'adresse IP, l'adresse MAC et le nom d'hôte uniquement après connexion de l'utilisateur.

   Après la connexion de l'utilisateur

   Spécifie que l'inventaire est collecté uniquement lorsque l'utilisateur se connecte après la RAC. Les logiciels réinstallés et les informations d'unités clientes sont signalés une fois que l'utilisateur s'est connecté.

   La collecte de l'inventaire après RAC se produit selon la configuration que vous avez spécifiée.

Balisage du modèle et création d'un cliché ou d'un vDisk

Le balisage vous permet d'assurer le suivi de la version du modèle utilisé par les ordinateurs de bureau virtuels. Balisez le modèle afin de générer une balise de modèle et d'associer les ordinateurs de bureau virtuels à leur modèle Or parent.

Procédez comme suit:

1. Faites glisser la procédure Modèle de balise du package d'extension VDI de l'agent CA DSM vers le modèle Or dans l'explorateur DSM.

   Le statut de la procédure s'affiche après avoir exécuté cette dernière.

2. Réalisez l'une des actions suivantes selon la solution de virtualisation de bureaux virtuels :

   ■ (Pour XenDesktop avec les services de provisionnement Citrix) Créez le vDisk à l'aide de XenConvert ou d'un autre outil d'imagerie approprié.

   ■ (Pour VMware View et Citrix MCS) Arrêtez l'ordinateur virtuel et créez un cliché.

   Cette action permet d'associer le cliché ou le vDisk à la balise de modèle.

Le cliché ou le vDisk sont créés et associés au modèle Or à l'aide de la balise de modèle.

Vérification de l'affectation du modèle Or

Vous pouvez vérifier le modèle Or affecté en consultant les paramètres de modèle disponibles dans l'inventaire.

Procédez comme suit:

1. Sélectionnez Ordinateurs et utilisateurs, Tous les ordinateurs, *Nom de l'ordinateur*, Inventaire.

2. Cliquez sur l'onglet Système d'exploitation, Paramètres de modèle.

   La liste des modèles affectés s'affiche.

Le modèle Or est maintenant prêt pour la gestion des ordinateurs de bureau virtuels.

Stratégies de configuration pour la prise en charge de la virtualisation d'ordinateurs de bureau

Après avoir installé le package d'extension de prise en charge VDI de l'Agent CA DSM, configurez les stratégies de configuration Client Automation pour les ordinateurs de bureau virtuels. Certaines de ces stratégies sont obligatoires et sont prédéfinies par VMware View. D'autres sont facultatives et requièrent la saisie d'informations comme indiqué.

Un nouveau groupe de stratégies d'enregistrement est ajouté et d'autres groupes de stratégie de configuration sont étendus pour prendre en charge la gestion des ordinateurs de bureau virtuels fournis par Citrix XenDesktop et VMware View.

Remarque : Appliquez les stratégies de configuration aux agents des ordinateurs de bureau virtuels clonés et aux agents des modèles Or. Ce processus, à l'exception des stratégies obligatoires gérées localement et prédéfinies par les scripts de clonage, doit être réalisé avant d'enregistrer le cliché de modèle Or.

La stratégie n'est pas héritée automatiquement par les ordinateurs de bureau virtuels clonés à partir du modèle Or. Lorsque les valeurs des ordinateurs de bureau virtuels clonés et celles des stratégies gérées de manière centralisée sont différentes, les valeurs sont écrasées peu après l'enregistrement auprès du gestionnaire.

Groupe de stratégies d'enregistrement

Un nouveau sous-groupe de stratégies, à savoir les stratégies d'enregistrement, a été ajouté sous le groupe de stratégies Composants communs pour l'identification spécifique des ordinateurs de bureau virtuels. Le groupe de stratégies d'enregistrement contient les stratégies suivantes :

Clé de l'hôte

Définit une chaîne utilisée pour identifier de façon univoque un ordinateur cloné. Une clé d'hôte est requise pour les clones liés car chaque recomposition de l'ordinateur de bureau virtuel génère un nouvel ordinateur virtuel qui enregistre un nouvel ordinateur unique dans la MDB. Par conséquent, au fil du temps, le gestionnaire de domaines détecterait de nombreux ordinateurs qui n'existeraient plus. Si la clé d'hôte est utilisée, les enregistrements d'ordinateurs existants pour les ordinateurs de bureau virtuels dans la MDB sont réutilisés.

Une clé hôte contient le texte brut et des macros. A l'enregistrement, CAF développe les macros et envoie le résultat au serveur de modularité. Le moteur utilise alors la clé d'hôte plutôt que le nom/l'UUID/l'adresse de l'hôte pour identifier les actifs dans la MDB. Désormais, la clé de l'hôte identifie l'agent.

Remarque : Dans les scénarios classiques, l'adresse d'ordinateur n'est pas changée pendant la recomposition des clones liés persistants. Il arrive toutefois dans certains cas que VMware modifie l'adresse des clones liés persistants pendant l'opération de recomposition. Par conséquent, l'utilisation d'une clé d'hôte est généralement requise aussi bien pour des clones liés persistants et non persistants que pour des ordinateurs de bureau virtuels MCS.

Utilisez les macros suivantes :

Variable d'environnement : $env(name)

Exemple : $env(“COMPUTERNAME")-VDI

Clé de registre : $reg(key,value)

Exemple : $reg(“HKLM\SOFTWARE\CA\GuestID”, ”GuestUUID”)-VDI

Valeur de fichier INI : $ini(path,section,key)

Exemple : $ini(“c:\id.ini”,”identity”,”uuid”)-VDI

Vous pouvez également combiner ces macros dans la même chaîne.

Exemple : $env(“COMPUTERNAME")-
$reg(“HKLM\SOFTWARE\CA\GuestID”,”GuestUUID”)-VDI

Remarque : Par défaut, le script CAFPostInit.dms définit la clé d'hôte sur l'agent avec $env(“COMPUTERNAME”). Vous ne devez donc pas modifier cette stratégie. Toutefois, si vous voulez utiliser une autre macro, vérifiez que toutes les clés d'hôte générées sont uniques à l'aide des chaînes de macro de clé d'hôte appropriées dans le script CAFPostInit.dms. Vérifiez aussi que la clé d'hôte ne compte pas plus de 64 caractères.

Valeur par défaut : vide, <géré localement>

Configuration des serveurs de modularité

Permet à l'administrateur de configurer le serveur de modularité de l'agent, qui est basé sur le modèle de nommage d'ordinateur virtuel utilisé pour le pool et la plage d'ordinateurs de bureau. Vous pouvez appliquer plusieurs plages. Cette stratégie est facultative. Si aucune valeur n'est définie, tous les clones rendent compte au même serveur de modularité que l'agent du modèle Or à partir duquel ils ont été clonés. Pour plus d'informations, consultez la rubrique Configuration des serveurs de modularité.

Groupe de stratégies Agent (Software Delivery)

Le groupe de stratégie Agent (Software Delivery) a été développé pour inclure les stratégies de configuration suivantes en vue de la gestion de l'agent Software Delivery dans des environnements VMware View.

Remarque : Les stratégies de configuration de réinstallation après un arrêt brutal dans le groupe de stratégies Agent s'appliquent uniquement à la réinstallation hors ligne après un arrêt brutal. La fonctionnalité traditionnelle de réinstallation après un arrêt brutal est configurée par les stratégies du groupe de stratégies Gestionnaire Software Delivery.

Vous pouvez modifier les valeurs des paramètres des stratégies en double-cliquant sur une stratégie, afin d'afficher la boîte de dialogue Propriétés des paramètres.

Réinstallation après un arrêt brutal : comportement des entrées multiples de la même procédure d'activation ou de configuration

Détermine si les procédures logicielles dupliquées sont exclues pendant la réinstallation hors ligne après un arrêt brutal.

Software Delivery ne permet qu'une seule exécution des procédures d'installation, mais autorise plusieurs exécutions des procédures d'activation et de configuration. Lorsque l'agent prépare le conteneur de réinstallation après un arrêt brutal pour un package logiciel, plusieurs procédures d'activation et de configuration peuvent être incluses. La valeur définie pour cette stratégie détermine le mode de gestion des procédures d'activation ou de configuration dupliquées dans un package logiciel unique. Les valeurs valides sont les suivantes :

Réexécuter toutes les procédures d'activation ou de configuration dupliquées

Indique que toutes les procédures d'activation ou de configuration enregistrées dans la base de données sont exécutées.

Réexécuter uniquement la première procédure d'activation ou de configuration dupliquée

Indique que si des procédures d'activation ou de configuration sont incluses plusieurs fois, seule la première procédure dupliquée est exécutée.

Réexécuter uniquement la dernière procédure d'activation ou de configuration dupliquée

Indique que si des procédures d'activation ou de configuration sont incluses plusieurs fois, seule la dernière procédure dupliquée est exécutée.

Valeur par défaut : Réexécuter toutes les procédures d'activation ou de configuration dupliquées

Réinstallation après un arrêt brutal : type de conteneur

Spécifie si l'agent exécute les jobs logiciels dans le conteneur de réinstallation hors ligne après un arrêt brutal comme un lot ou sans lien. Les valeurs valides sont les suivantes :

Lot

Indique que tous les jobs doivent être exécutés de façon séquentielle comme une unité unique de travail pour chaque cible. Si un job de la séquence échoue, les jobs restants pour cette cible ne sont pas exécutés.

Sans liaison

Indique que les jobs doivent être exécutés de façon séquentielle, mais indépendamment les uns des autres.

Valeur par défaut : Lot

Réinstallation après un arrêt brutal : supprimer la procédure logicielle de la base de données des états de logiciel en cas d'échec

Détermine si la base de données des états de logiciel est mise à jour lorsqu'un ou plusieurs jobs dans le conteneur de réinstallation après un arrêt brutal (RAC) échoue. Si cette stratégie est définie sur True, les entrées de job échoué sont supprimées de la base de données des états de logiciel. Si elle est définie sur False, les entrées de job échoué sont conservées.

Valeur par défaut : True

Réinstallation après un arrêt brutal : laisser le job vérifier l'interface utilisateur graphique jusqu'à sa fermeture par l'utilisateur final

Détermine si la boîte de dialogue Vérification des jobs de livraison de logiciels DSM reste ouverte jusqu'à ce que l'utilisateur la ferme en cas d'échec de la réinstallation après un arrêt brutal pendant une réinstallation en mode interactif. Par exemple, la définition de cette stratégie sur la valeur True garantit que l'utilisateur ne manquera pas une notification d'échec de la réinstallation après un arrêt brutal s'il s'éloigne de son ordinateur.

Valeur par défaut : True

Réinstallation après un arrêt brutal : maintenir la base de données des états de logiciel de préinstallation

Indique si une base de données des états de logiciel de préinstallation est tenue à jour lorsqu'aucun utilisateur n'est affecté aux ordinateurs de bureau virtuels. Une base de données des états de logiciel de préinstallation est utile lorsque des ordinateurs de bureau virtuels dans un pool sont créés et enregistrés en tant qu'agents, mais pas encore affectés à des utilisateurs. Une base de données de préinstallation permet à l'administrateur d'appliquer les packages logiciels requis aux ordinateurs de bureau virtuels.

Si cette stratégie est définie sur True, une base de données des états de logiciel de préinstallation est tenue à jour sur le système local de fichiers tant qu'aucun utilisateur n'est affecté à l'ordinateur de bureau virtuel. La base de données de préinstallation est fusionnée avec la base de données des états de logiciel d'instance d'utilisateurs affectés quand l'utilisateur se connecte pour la première fois.

Si cette stratégie est définie sur False, les conditions suivantes s'appliquent.

Ordinateurs de bureau persistants :

pour les ordinateurs de bureau persistants, si la réinstallation hors ligne après un arrêt brutal est configurée pour s'exécuter à la connexion, la définition de cette stratégie sur False entraîne la réinstallation de ces packages logiciels, car les enregistrements de job logiciel sont ajoutés à la base de données des instances plutôt qu'à la base de données de préinstallation.

Ordinateurs de bureau non persistants :

pour les ordinateurs de bureau non persistants, la définition de cette stratégie sur False a pour conséquence que les enregistrements de job de livraison de logiciels ne sont pas maintenus pour ces packages logiciels. En outre, ils ne peuvent pas être réinstallés lorsque l'ordinateur de bureau virtuel est actualisé par la suite.

Valeur par défaut : True

Réinstallation après un arrêt brutal : maintenir la base de données des états de logiciel

Indique si l'agent Software Delivery maintient une base de données de son état, indépendamment de la fonctionnalité VMware View.

Remarque : Cette stratégie est obligatoire et prédéfinie sur True par les scripts d'intégration VMware View. Ne changez pas manuellement la valeur définie.

Valeur par défaut : False, <géré localement>

Réinstallation après un arrêt brutal : nombre maximum de secondes pour une nouvelle tentative

Définit le nombre maximum de secondes qu'un agent peut être en veille entre deux tentatives de contact avec le serveur de modularité lors d'une vérification des jobs. Cette stratégie fonctionne avec la stratégie Réinstallation après un arrêt brutal : nombre de tentatives en cas de réinstallation hors ligne après un arrêt brutal. Les tentatives de reconnexion se poursuivent jusqu'à ce que la limite spécifiée par l'une de ces stratégies soit atteinte.

Valeur par défaut : 60

Réinstallation après un arrêt brutal : nombre de tentatives en cas de réinstallation hors ligne après un arrêt brutal

Définit le nombre maximum de nouvelles tentatives de connexion au serveur de modularité qu'un agent peut effectuer pendant une vérification des jobs. Cette stratégie fonctionne avec la stratégie Réinstallation après un arrêt brutal : nombre maximum de secondes pour une nouvelle tentative. Les tentatives de reconnexion se poursuivent jusqu'à ce que la limite spécifiée par l'une de ces stratégies soit atteinte.

Valeur par défaut : 100

Réinstallation après un arrêt brutal : mot de passe pour l'accès à la base de données des états de logiciel d'instance

Spécifie le mot de passe de l'utilisateur autorisé à accéder à la base de données des états de logiciel d'instance. La chaîne du mot de passe est chiffrée. Si cette valeur est spécifiée, l'agent utilise ces informations d'identification pour accéder au partage réseau.

Il est recommandé de commencer par chiffrer le mot de passe à l'aide de la commande sd_acmd chiffrer. Ensuite, spécifiez le mot de passe chiffré comme l'un des paramètres lors de l'exécution du script Compose.bat qui, à son tour, définit le paramètre de configuration.

De même, si le mot de passe correspondant à l'emplacement de partage est le même pour tous les pools d'ordinateurs de bureau à créer à partir d'un cliché de modèle Or spécifique, vous pouvez définir le mot de passe dans la stratégie de configuration. Appliquez ensuite la stratégie au modèle Or et aux ordinateurs de bureau virtuels clonés.

Valeur par défaut : vide, <géré localement>

Réinstallation après un arrêt brutal : chemin d'accès à la base de données des états de logiciel d'instance

Spécifie le chemin d'installation de la base de données des états de logiciel d'instance. Le chemin d'accès spécifié peut inclure des variables d'environnement intégrées, par exemple, “\\Fileserver1\Share1\%COMPUTERNAME%\InstanceSoftwareDatabase”.

Remarque : Cette stratégie est obligatoire, mais vous devez entrer le chemin d'accès manuellement comme l'un des paramètres lors de l'exécution du script Compose.bat. Ce script définit à son tour le paramètre de configuration.

Valeur par défaut : vide, <géré localement>

Réinstallation après un arrêt brutal : chemin d'accès à la base de données des états de logiciel de modèle

Spécifie le chemin d'installation de la base de données des états de logiciel de modèle. Si la valeur est vide, l'agent utilise le chemin d'accès spécifique à l'unité approprié, c'est-à-dire <répertoire_installation_ITCM>\SD\ASM\DATABASE\Agent\TemplateSoftwareDatabase.

Valeur par défaut : vide, <géré localement>

Réinstallation après un arrêt brutal : paramètre de stratégie de réinstallation après un arrêt brutal de l'agent

Contrôle le paramètre Stratégie RAC de l'agent Software Delivery. Si cette stratégie est définie sur True, la stratégie RAC de l'agent est définie sur Hors ligne. Si elle est définie sur False, la stratégie RAC est définie sur le paramètre RAC par défaut.

Remarque : Cette stratégie est obligatoire et prédéfinie sur True par les scripts d'intégration VMware View. Ne changez pas manuellement la valeur définie.

La valeur définie ici est par défaut celle spécifiée sous l'onglet Software Delivery de la boîte de dialogue Propriétés de l'ordinateur.

Valeur par défaut : False, <géré localement>

Réinstallation après un arrêt brutal : définir l'agent SD pour le mode de modèle Or

Permet à l'agent d'établir une distinction entre l'exécution sur un modèle Or ou un clone. Si cette stratégie est définie sur True, l'agent s'exécute sur un modèle Or.

Remarque : Cette stratégie est obligatoire et prédéfinie par les scripts d'intégration VMware View.

Valeur par défaut : False, <géré localement>

Réinstallation après un arrêt brutal : nom d'utilisateur pour l'accès à la base de données des états de logiciel d'instance

Spécifie le nom de l'utilisateur autorisé à accéder à la base de données des états de logiciel d'instance. Le nom d'utilisateur doit présenter le format suivant : (*nom_domaine* | local\)'user'. La chaîne est chiffrée. Si cette valeur est spécifiée, l'agent utilise ces informations d'identification pour accéder au partage réseau.

Il est recommandé de commencer par chiffrer le nom d'utilisateur à l'aide de la commande sd_acmd encrypt. Spécifiez ensuite le nom d'utilisateur chiffré comme l'un des paramètres lors de l'exécution du script Compose.bat qui, à son tour, définit le paramètre de configuration.

De même, si le nom d'utilisateur correspondant à l'emplacement de partage est le même pour tous les pools d'ordinateurs de bureau à créer à partir d'un cliché de modèle Or spécifique, vous pouvez définir le nom d'utilisateur dans la stratégie de configuration. Appliquez ensuite la stratégie au modèle Or et aux ordinateurs de bureau virtuels clonés.

Remarque : Par défaut, lorsqu'un dossier est partagé, ses autorisations incluent uniquement le groupe "Tout le monde" avec des autorisations d'accès en lecture. Pour garantir que la base de données des états de logiciel d'instance est enregistrée sur un réseau, le partage réseau doit également inclure l'utilisateur mentionné ici dans l'onglet Autorisations de partage avec un droit d'accès Contrôle absolu (écriture).

Valeur par défaut : vide, <géré localement>

Groupe de stratégies Général (CAF)

Le groupe de stratégies Général (CAF) inclut les stratégies de configuration suivantes.

CAF : script de pré-initialisation

Spécifie le script que vous voulez exécuter lors du démarrage de caf et de l'initialisation. Le script est exécuté avant que l'UUID soit vérifié et avant que tous les modules d'extension soient démarrés.

CAF : script de post-initialisation

Spécifie le script que vous voulez exécuter après l'initialisation de caf. Le script est exécuté une fois que tous les modules d'extension ont démarré, mais avant leur premier enregistrement.

CAF : délai (en secondes) du script de pré-initialisation

Spécifie le délai d'attente en secondes observé par caf avant de terminer le script de pré-initialisation.

CAF : délai (en secondes) du script de post-initialisation

Spécifie le délai d'attente en secondes observé par caf avant de terminer le script de post-initialisation.

CAF : activer l'enregistrement au démarrage

Spécifie si le cadre d'applications communes (CAF) s'enregistre immédiatement auprès du gestionnaire de domaines lors du démarrage.

Valeur par défaut : True

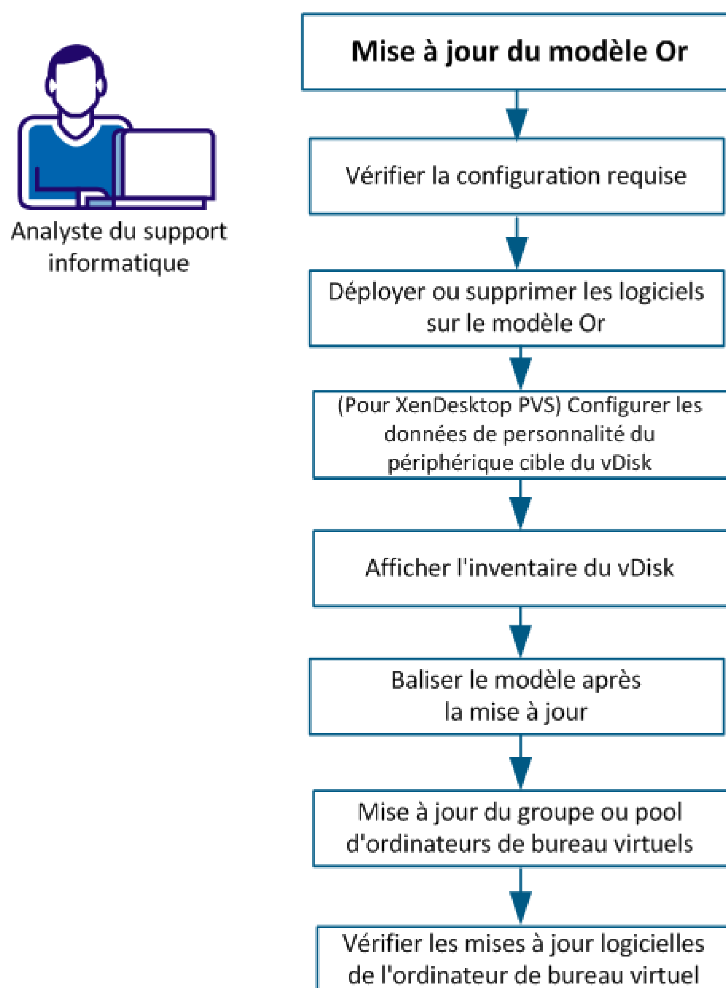
Important : Cette stratégie doit être configurée de sorte à être gérée localement avant l'installation du package d'extension de prise en charge VDI de l'agent CA DSM pour Windows FRA. Vous pouvez également cliquer avec le bouton droit de la souris sur la stratégie et sélectionner Géré localement dans le menu contextuel.

Remarque : Cette stratégie s'applique uniquement aux ordinateurs de bureau virtuels basés sur VMWare View et si le package d'extension de prise en charge VDI de l'agent CA DSM pour Windows FRA de la version antérieure à la version 12.5 SP1 Feature Pack 1 est utilisé.

Mise à jour du modèle Or

En tant qu'analyste du support informatique, vos responsabilités comprennent la mise à jour des modèles Or lorsque vous voulez ajouter ou supprimer des packages logiciels du modèle Or. La mise à jour des modèles Or permet de mettre à jour le clone VMWare View, l'ordinateur de bureau virtuel diffusé en continu par Citrix PVS ou l'ordinateur de bureau virtuel basé sur MCS.

Le diagramme suivant illustre les étapes permettant de mettre à jour le modèle Or :



Effectuez les tâches suivantes pour mettre à jour le modèle Or :

1. Vérification de la configuration requise (page 325)
2. Déploiement des logiciels sur le modèle Or (page 325)
3. Configuration des données de personnalité du périphérique cible du vDisk (page 326)
4. Affichage de l'inventaire du vDisk (page 328)
5. Balisage du modèle après la mise à jour (page 329)
6. Mise à jour du groupe ou pool d'ordinateurs de bureau virtuels (page 330)
7. Vérification des mises à jour logicielles de l'ordinateur de bureau virtuel (page 331)

Vérification de la configuration requise

Pour mettre à jour le modèle Or, vérifiez la configuration requise suivante :

- Vérifiez que vous avez déjà préparé et déployé un ou plusieurs modèles Or.
- Vérifiez que l'agent de bureau virtuel est installé sur l'ordinateur du modèle Or.

  Remarque : Ce scénario requiert une bonne maîtrise pratique des solutions de bureau virtuel telles que VMware View et Citrix XenDesktop.
- Vérifiez que le périphérique cible Citrix PVS est installé si vous voulez créer des ordinateurs de bureau virtuels Citrix utilisant un vDisk.

Déploiement ou suppression de logiciels sur le modèle Or

Vous pouvez déployer ou supprimer des packages logiciels du modèle Or de l'une des manières suivantes :

- Effectuez les modifications directement sur l'ordinateur du modèle Or. Cette méthode est valable pour les ordinateurs VMWare View et Citrix MCS basés sur des clichés.

- Mettez à jour un vDisk créé à partir du modèle Or. Cette méthode est valable pour les ordinateurs de bureau virtuels Citrix XenDesktop diffusés en continu par les services de provisionnement Citrix. Les considérations suivantes s'appliquent :
  - Le vDisk doit être démarré en mode privé sur un ordinateur ayant la même configuration que l'ordinateur du modèle Or.
  - Des données de personnalité sont affectées au périphérique cible utilisé pour démarrer le vDisk en mode privé sur le serveur de provisionnement Citrix afin d'indiquer que le vDisk est démarré pour la gestion des modèles. Pour plus d'informations sur les données de personnalité, reportez-vous à la rubrique Configuration des données de personnalité du périphérique cible du vDisk (page 326).
  - Lorsque vous démarrez le vDisk en mode privé pour la première fois, le vDisk est ajouté en tant qu'entité gérée dans Client Automation. Vous pouvez ensuite déployer ou supprimer des packages du vDisk à l'aide de la livraison de logiciels.
  - Le vDisk s'affiche sous forme d'enregistrement d'ordinateur dans l'explorateur DSM, sous Tous les ordinateurs, avec la convention de nommage suivante :

    <nom_batterie>-<nom_magasin>-<nom_vDisk>

    Si l'enregistrement d'ordinateur est introuvable dans l'explorateur DSM, reportez-vous à la rubrique Enregistrement du vDisk introuvable dans l'explorateur DSM.
  - Le même enregistrement d'ordinateur est utilisé pour le vDisk à chaque fois que vous démarrez le vDisk en mode privé sur un ordinateur pour la gestion des modèles.
  - Si l'ordinateur qui héberge le vDisk en mode privé est déjà un ordinateur géré dans Client Automation, les déploiements logiciels sont uniquement effectués sur le vDisk et non sur l'ordinateur.

    Remarque : Lorsque l'ordinateur a démarré avec le vDisk en mode privé, tous les jobs logiciels sont en attente jusqu'à ce que l'ordinateur démarre avec le lecteur local.

Remarque : Vous pouvez également mettre à jour le modèle Or, créer un vDisk à partir de ce dernier ou remplacer un vDisk existant pour mettre à jour les ordinateurs de bureau virtuels.

(Pour XenDesktop PVS) Configuration des données de personnalité du périphérique cible du vDisk

Configurez les données de personnalité du périphérique cible du vDisk dans la console du serveur de provisionnement afin que Client Automation puisse traiter le vDisk démarré en mode privé comme un modèle Or.

Procédez comme suit:

1. Dans la console des services de provisionnement Citrix, ouvrez la boîte de dialogue des propriétés du périphérique cible auquel le vDisk est affecté.
2. Cliquez sur l'onglet Personality et ajoutez les paramètres suivants :

   CA_DSM_GoldenTemplate

   Indique si le vDisk est un modèle Or ou un ordinateur de bureau virtuel en mode privé. Définissez la valeur de ce paramètre comme True.

   ProvisioningServer

   Spécifie l'adresse IP ou le nom d'hôte du serveur de provisionnement.

   ProvisioningServicesUser

   Spécifie le nom de l'utilisateur ayant accès à la batterie de serveurs des services de provisionnement ou celui de l'utilisateur indiqué lors de la connexion à la console du serveur de provisionnement. Chiffrez le nom de l'utilisateur à l'aide de la commande sd_acmd encrypt et transférez la valeur chiffrée.

   ProvisioningServicesPassword

   Spécifie le mot de passe de l'utilisateur des services de provisionnement. Chiffrez le mot de passe à l'aide de la commande sd_acmd encrypt et transférez la valeur chiffrée.

   ProvisioningServerPort

   Spécifie le port du serveur de provisionnement sur lequel le service SOAP s'exécute. La valeur par défaut est 54321.

   Remarque : Transférez les paramètres du serveur de provisionnement en tant que paramètres d'utilisateur dans le package d'extension de prise en charge VDI de l'agent CA DSM tout en appliquant le mode d'installation du modèle sur le modèle Or. Utilisez le format suivant:

   ```
   /pvsserver:<adresse_IP_serveur/nom> /pvsuser:<nom_utilisateur_chiffré>
   /pvspwd:<mot_de_passe_chiffré> /portno:<numéro_port>
   ```

3. Enregistrez les changements.

   Les données de personnalité du périphérique cible du vDisk sont configurées comme un modèle Or.

Affichage de l'inventaire du vDisk

Après le démarrage du vDisk en mode privé, celui-ci est ajouté en tant qu'entité gérée dans Client Automation. Voici un exemple pour Citrix XenDesktop.

Procédez comme suit: (dans l'explorateur DSM) :

1. Sélectionnez Ordinateurs et utilisateurs, Tous les ordinateurs, *nom_vDisk,* Inventaire, noeud Système d'exploitation.

   nom_vDisk

   Spécifie le nom du vDisk au format suivant : *nom_batterie-nom_magasin-nom_vDisk*.

2. Sélectionnez le sous-dossier Paramètres de modèle pour afficher les valeurs des attributs suivants :

   IsGoldenTemplate

   Indique si un agent est un modèle Or (True) ou un ordinateur de bureau virtuel (False). La valeur est définie sur True lorsqu'un vDisk principal ou le clone d'un vDisk principal est démarré en mode privé pour la gestion des modèles.

   TemplateHostUUID

   Spécifie l'UUID d'hôte du modèle Or. L'UUID d'hôte pour un vDisk principal est le modèle Or et, pour un vDisk cloné, le vDisk principal.

   Pour plus d'informations, reportez-vous à la rubrique Gestion des clones de vDisk. (page 331)

   TemplateName

   Spécifie le nom du modèle Or.

   TemplateTag

   Indique la date et l'heure du dernier balisage du modèle Or.

3. Cliquez sur le noeud Historique des modèles pour afficher l'historique des modèles du vDisk. Vous pouvez consulter l'historique des mises à jour du modèle Or.

4. Cliquez sur Virtualisation, vDisks Citrix Xen.

   La batterie de serveurs, le magasin et le site du vDisk s'affichent.

Procédez comme suit: (dans la console Web) :

1. Accédez à Ordinateurs, Inventaire, Inventaire des actifs détectés et cliquez sur Système d'exploitation.
2. Sous l'onglet Plus de détails, cliquez sur Paramètres de modèle pour afficher les valeurs des attributs IsGoldenTemplate, TemplateName, TemplateTag et TemplateHostUUID.
3. Sous l'onglet Plus de détails, cliquez sur Historique des modèles pour afficher l'historique des modèles.

Vous avez vérifié les informations de relation et l'historique des modèles.

Balisage du modèle après la mise à jour

Le balisage vous permet d'assurer le suivi de la version du modèle utilisé par les ordinateurs de bureau virtuels. Balisez le modèle afin de générer une balise de modèle et d'associer les clones à leur modèle Or parent.

Procédez comme suit:

1. Effectuez un glisser-déposer de la procédure Modèle de balise à partir du package d'extension VDI de l'agent CA DSM sur le modèle Or dans l'explorateur DSM.
2. Réalisez *l'une* des actions suivantes selon la solution de bureau virtuel :
   - (Pour XenDesktop basé sur Citrix PVS) Arrêtez l'ordinateur afin que les mises à jour soient enregistrées sur le vDisk.
   - (Pour VMware View et Citrix MCS) Arrêtez l'ordinateur virtuel et créez un cliché.

     Cette action permet d'associer le cliché à la balise de modèle.

Mise à jour du groupe ou pool d'ordinateurs de bureau virtuels

Mettez à jour le groupe ou pool d'ordinateurs de bureau virtuels qui utilise le modèle Or que vous avez mis à jour. Pour plus d'informations sur la mise à jour du groupe ou pool d'ordinateurs de bureau virtuels, consultez la documentation de VMware View ou Citrix XenDesktop. Une fois le groupe ou pool d'ordinateurs de bureau virtuels mis à jour, les mises à jour du modèle Or s'appliquent aux ordinateurs de bureau virtuels lors du redémarrage suivant.

Affectez le vDisk mis à jour ou le cliché aux ordinateurs de bureau virtuels pour propager les mises à jour du modèle Or lors du redémarrage suivant.

Procédez comme suit: (pour VMware View) :

1. Arrêtez le modèle Or.
2. Créez un cliché du modèle Or.
3. Recomposez le pool à l'aide du nouveau cliché.

Procédez comme suit: (pour les ordinateurs de bureau virtuels basés sur Vdisk) :

1. Arrêtez l'ordinateur du vDisk.
2. Supprimez l'affectation du vDisk de l'ordinateur.
3. Faites passer le vDisk en mode standard ou différentiel.
4. Affectez le vDisk mis à jour aux ordinateurs de bureau virtuels.
5. Redémarrez les ordinateurs de bureau virtuels ; dans le cas contraire, les modifications prennent effet lorsqu'ils redémarrent.

   Remarque : Vous pouvez affecter le vDisk mis à jour aux ordinateurs de bureau virtuels à l'aide de la fonctionnalité automatique de mises à jour incrémentielles du vDisk ou celle des services de provisionnement Citrix.

Procédez comme suit: (pour les ordinateurs de bureau virtuels basés sur MCS) :

1. Arrêtez le modèle Or.
2. Créez un cliché du modèle Or.
3. Mettez à jour le catalogue En pool à l'aide du nouveau cliché.

Vérification des mises à jour logicielles de l'ordinateur de bureau virtuel

Affichez le logiciel d'ordinateur de bureau virtuel afin de vérifier si les mises à jour effectuées sur le modèle Or sont disponibles sur les ordinateurs de bureau virtuels.

Procédez comme suit:

1. Sélectionnez Ordinateurs et utilisateurs, Tous les ordinateurs, *Ordinateur de bureau virtuel,* Logiciel(s), noeud Packages installés.

   Dans le volet de droite, vérifiez si les modifications que vous avez apportées au modèle Or ou au vDisk apparaissent sur l'ordinateur de bureau virtuel.

Les mises à jour du modèle Or ont été effectuées.

Gestion des vDisk et des clones de vDisk

En tant qu'analyste du support informatique, vous devez comprendre la manière dont Client Automation gère la relation entre le vDisk et ses clones.

Ce scénario décrit la façon dont Client Automation gère les vDisk et les clones.

Gestion des clones de vDisk

Vous pouvez copier ou cloner les vDisks pour provisionner des ordinateurs de bureau virtuels. Les copies ou clones de vDisk et leur vDisk parent s'affichent dans la MDB sous forme d'enregistrements de gestion distincts. Les valeurs comstore de la batterie de serveurs de provisionnement, du magasin, du site et du nom du vDisk permettent de distinguer un vDisk parent d'un vDisk cloné.

Client Automation utilise les règles suivantes pour identifier les clones de vDisk et créer un enregistrement de gestion distinct :

- Lorsqu'un vDisk est démarré en mode privé pour la gestion des modèles, un nouvel enregistrement de gestion est créé dans Client Automation et le nom de l'agent est au format *nom_batterie-nom_magasin-nom_vDisk*.
- Lorsqu'un clone de vDisk est démarré en mode privé pour la gestion des modèles à partir d'une batterie de serveurs différente, un nouvel enregistrement de gestion est créé pour le clone.
- Lorsque le clone est démarré à partir de la même batterie de serveurs, mais d'un magasin différent, alors que le vDisk et son nom parent sont différents, un nouvel enregistrement de gestion est créé pour la copie du vDisk.
- Un nouvel enregistrement de gestion est créé pour la copie du vDisk selon la règle suivante :
    - Le vDisk clone est démarré à partir de la même batterie de serveurs, mais à partir d'un magasin différent.
    - Le nom du vDisk et de son parent sont identiques.
    - Le site à partir duquel le vDisk est démarré pour la gestion des modèles et celui de son parent sont différents.

      Remarque : Si le site est identique à celui du vDisk parent, l'administrateur est invité à vérifier s'il faut créer un enregistrement de gestion dans la MDB ou réutiliser l'enregistrement existant.
- Un nouvel enregistrement de gestion est créé selon la règle suivante :
    - La batterie de serveurs et le magasin sont identiques.
    - Le nom du vDisk change.
    - Le vDisk parent fait partie du magasin.
    - Le vDisk est démarré en tant que copie.

      Remarque : Si le vDisk parent ne fait pas partie du magasin, l'administrateur est invité à vérifier s'il faut créer un enregistrement de gestion dans la MDB ou réutiliser l'enregistrement existant.
- Lorsque les noms du vDisk, de la batterie de serveurs et du magasin sont identiques, un enregistrement d'ordinateur géré existant est réutilisé.

Affichage de la relation entre le modèle Or, le vDisk principal et les clones

Pour identifier le vDisk à partir duquel un vDisk particulier a été dérivé, Client Automation collecte l'inventaire sous Paramètres de modèle et Historique des modèles.

A l'aide de ces informations d'inventaire, vous pouvez identifier le parent immédiat d'un vDisk particulier et l'historique des modifications apportées au vDisk. La relation est identifiée comme suit :

- Un vDisk principal pointe vers le modèle Or en tant que parent.
- Si vous avez créé un clone à partir d'un vDisk principal après avoir démarré celui-ci en mode privé, le clone pointe vers le vDisk principal en tant que parent.
- Si vous avez créé un clone à partir d'un vDisk principal avant de démarrer celui-ci en mode privé, le clone est identique au vDisk principal et pointe vers le modèle Or en tant que parent. Si d'autres clones sont créés à partir de ces clones du vDisk principal, tous les clones pointent vers le modèle Or en tant que parent.

Procédez comme suit: (dans l'explorateur DSM) :

1. Sélectionnez Ordinateurs et utilisateurs, Tous les ordinateurs, nom_vDisk, Inventaire, dossier Système d'exploitation.
2. Sélectionnez le sous-dossier Paramètres de modèle pour afficher les valeurs des attributs suivants :

   IsGoldenTemplate

   Indique si l'agent en question est un modèle Or (True) ou un ordinateur de bureau virtuel (False). La valeur est True pour le vDisk principal et ses clones.

   TemplateHostUUID

   Spécifie l'UUID d'hôte du modèle Or. Pour un vDisk principal, l'UUID d'hôte est celui du modèle Or. Pour les vDisk clonés, l'UUID d'hôte diffère en fonction des facteurs suivants :

   - Si le clone a été créé après le démarrage en mode privé du vDisk principal, l'UUID d'hôte est celui du vDisk principal.
   - Si le clone a été créé avant le démarrage en mode privé du vDisk principal, l'UUID d'hôte est celui du système du modèle Or.

   TemplateName

   Spécifie le nom du modèle Or.

   TemplateTag

   Indique la date et l'horodatage du modèle pour le modèle Or ou le vDisk uniquement si le modèle a été balisé.
3. Sélectionnez le sous-dossier Historique des modèles pour afficher l'historique des modèles de l'ordinateur de bureau virtuel ou des modèles, pour autant que ces derniers aient été balisés.

Procédez comme suit: (dans la console Web) :

1. Sélectionnez Ordinateurs, Inventaire, page Inventaire des actifs détectés.
2. Cliquez sur l'onglet Système d'exploitation pour afficher la valeur de l'attribut Ordinateur virtuel.
3. Sous l'onglet Plus de détails, cliquez sur Paramètres de modèle pour afficher les valeurs des attributs IsGoldenTemplate, TemplateName, TemplateTag et TemplateHostUUID.
4. Sous l'onglet Plus de détails, cliquez sur Historique des modèles pour afficher l'historique des modèles du clone.

   Vous avez vérifié les informations de relation et l'historique des modèles.

Gestion des ordinateurs de bureau virtuels à partir de Client Automation

En tant qu'analyste du support informatique, vos responsabilités comprennent la gestion des ordinateurs de bureau virtuels à partir de Client Automation. La gestion des ordinateurs de bureau virtuels inclut le déploiement de logiciels ou de patchs sur les ordinateurs de bureau virtuels et la collecte de l'inventaire à partir de ceux-ci. Vous devez également tenir compte de la manière dont Client Automation réinstalle les logiciels sur les ordinateurs de bureau et du moment auquel le programme effectue cette opération.

Remarque : Les opérations de déploiement des packages logiciels et de collecte de l'inventaire à partir d'ordinateurs de bureau virtuels sont similaires à celles effectuées sur tout autre ordinateur dans Client Automation.

Directives d'implémentation pour les ordinateurs de bureau virtuels

Pour les packages logiciels installés sur des ordinateurs de bureau virtuels plutôt que sur le modèle Or, vous devez tenir compte des restrictions et des directives suivantes :

- Les packages qui ne sont pas stockés sur un média intermédiaire dans la bibliothèque de logiciels du serveur de modularité sur lequel l'agent est enregistré, ne sont pas réinstallés.
- La réinstallation n'est pas prise en charge pour les procédures ajoutées avec de nouveaux fichiers.
- Elle n'est pas prise en charge pour l'agent Profils d'utilisateur, mais l'est pour l'agent Ordinateur.

- Lorsqu'un ordinateur de bureau virtuel est extrait à l'aide de la fonctionnalité Offline Desktop de VMware View, puis l'extraction est annulée, tous les changements d'état de logiciel sont conservés dans la base de données de logiciels d'instance. Lorsque la réinstallation hors ligne après un arrêt brutal est effectuée, le logiciel est réinstallé, car il a été enregistré dans la base de données des états et n'a pas été supprimé pendant l'annulation. Par conséquent, le logiciel doit être désinstallé manuellement si vous ne voulez pas le conserver.
- L'envoi de jobs de livraison de logiciels avec les options de redémarrage, de déconnexion et d'arrêt activées n'est pas pris en charge pour les ordinateurs de bureau virtuels non persistants. Un ordinateur de bureau non persistant est uniquement lié à un utilisateur le temps de sa connexion. Lorsque l'utilisateur se connecte la fois suivante, vous pouvez l'allouer à un ordinateur de bureau différent. Ces options ne sont donc pas logiques dans ce cas.
- Les packages dont le transfert sur le réseau ou l'installation tarde un certain temps doivent être installés sur le modèle Or, plutôt que sur l'ordinateur de bureau virtuel. Dans le cas contraire, le délai de réinstallation devient inacceptable.
- Vous pouvez préstocker les applications virtualisées sur le modèle Or et les provisionner ultérieurement sur des ordinateurs de bureau virtuels par l'intermédiaire d'une installation autonome. De cette façon, l'utilisation de la bande passante réseau est réduite pendant la phase de recomposition ou d'actualisation et pendant l'utilisation.
- Vous pouvez obtenir un résultat similaire en utilisant des formats de package gérés, comme SXP, PIF et MSI, et avec quelques recherches et ajustements. Par exemple, SXP fournit un filtre d'utilisateur qui permet au package d'être installé sur le modèle Or. Toutefois, le filtre est uniquement mis à la disposition des utilisateurs de clones qui appartiennent à des groupes d'utilisateurs d'annuaire local ou actif spécifiques.
- Les applications virtualisées doivent être provisionnées sur des ordinateurs de bureau virtuels en mode de diffusion en continu. De cette façon, l'utilisation de la bande passante réseau est réduite pendant la phase de recomposition ou d'actualisation, mais pas pendant l'utilisation.
- Les applications qui stockent leur configuration en dehors du profil d'utilisateur ou des dossiers redirigés, ne conservent pas automatiquement leur configuration après la réinstallation. Les applications qui réinitialisent leur configuration plutôt que de l'hériter lors de l'installation sont également confrontées à ce problème.
- Si la base de données des états de logiciel de modèle et la base de données des états de logiciel d'instance contiennent des enregistrements du même logiciel, mais dans des versions différentes, la mise à niveau ou l'installation d'une version antérieure est effectuée lors de la réinstallation hors ligne après un arrêt brutal. L'administrateur est responsable de la configuration appropriée du système pour prévenir ce problème, particulièrement dans des scénarios d'installation d'une version antérieure.
- La méthode de téléchargement DTS n'est pas prise en charge pour les agents d'ordinateurs de bureau virtuels.

- Pour les pools d'ordinateurs de bureau non persistants, les réinstallations sont uniquement effectuées lorsqu'un utilisateur se connecte.
- Il est recommandé de désactiver le mode de profil d'utilisateur pour la fonctionnalité Software Delivery en cas de d'ordinateurs de bureau virtuels clones liés.

  Les profils d'utilisateur ne sont pas nécessaires dans cette situation, car une relation univoque existe entre l'utilisateur et l'ordinateur de bureau virtuel. L'activation des profils d'utilisateur engendre des communications supplémentaires entre l'agent et le serveur de modularité, ce qui peut affecter la modularité globale.

Réinstallation hors ligne après un arrêt brutal

La réinstallation hors ligne après un arrêt brutal est une tâche de réinstallation après l'arrêt brutal (RAC) effectuée par l'agent plutôt que par le gestionnaire. Les ordinateurs virtuels sont *recomposés* fréquemment, à savoir, chaque fois que le modèle Or est mis à jour et le disque réinitialisé ; toute modification apportée à l'ordinateur virtuel par rapport à la réinitialisation précédente est efficacement évitée. Dans le cas d'ordinateurs virtuels, l'agent (non le gestionnaire) est responsable de la création du conteneur de jobs RAC. Lors de la réinitialisation du disque, l'agent initialise une réinstallation hors ligne après un arrêt brutal pour restaurer tout logiciel déployé vers l'agent.

Pour la réinstallation hors ligne après un arrêt brutal, l'agent Software Delivery contient une base de données des états de logiciel basée sur le système de fichiers. Cette base de données contient les informations suivantes pour chaque package logiciel installé :

- La procédure utilisée pour installer le logiciel
- Toutes les procédures de configuration ou d'activation postérieures à l'installation pour l'ordinateur cible de l'agent uniquement.
- Toutes les informations spécifiques à un job, comme les paramètres d'utilisateur.

Cette base de données des états de logiciel est maintenue par l'agent Software Delivery et mise à jour à chaque exécution d'un job logiciel. En cas de désinstallation d'un package logiciel, les enregistrements correspondants sont supprimés. Lorsqu'elle est activée, la base de données des états de logiciel reflète toujours l'état actuel de la fonctionnalité Software Delivery pour l'agent.

En outre, elle hérite de l'historique d'installation du modèle Or sur lequel l'ordinateur de bureau virtuel se base. Par conséquent, elle est fractionnée en deux parties, l'une destinée à l'utilisation du modèle Or et l'autre à l'utilisation de l'instance clonée. La partie modèle de la base de données des états de logiciel est stockée sur le disque système du modèle Or. Tous les jobs logiciels ciblant le modèle Or utilisent uniquement cette base de données. Lorsque l'ordinateur de bureau virtuel est cloné, son agent utilise uniquement la base de données des états de logiciel d'instance pour suivre son état.

Le disque système d'un ordinateur de bureau virtuel cloné étant détruit lors d'une opération de recomposition ou d'actualisation, vous ne pouvez pas y stocker la base de données des états de logiciel d'instance. Cette base de données doit être stockée dans un autre emplacement, contrôlé par la stratégie de configuration commune, par exemple, sur le disque de données de l'utilisateur d'un clone lié VMware View ou sur un serveur de fichiers accessible à partir de l'ordinateur de bureau virtuel.

Important : Les administrateurs doivent garantir l'accessibilité ininterrompue de la base de données des états de logiciel lors de la gestion des jobs logiciels standard et lors de l'installation hors ligne, en particulier si la base de données de logiciels d'instance se trouve sur un partage réseau.

Informations complémentaires :

Groupe de stratégies Agent (Software Delivery) (page 316)

Statut de réinstallation

A la fin du processus de réinstallation, le gestionnaire de domaines est informé de la réussite ou de l'échec de chaque job. Le statut est également affiché dans la boîte de dialogue Vérification des jobs de livraison de logiciels DSM de l'agent lorsque la réinstallation hors ligne est en cours.

Si un job échoue ou si plusieurs jobs ne peuvent pas être exécutés à cause d'autres paramètres, tels que Exclure de la réinstallation après un arrêt brutal, la boîte de dialogue Vérification des jobs de livraison de logiciels DSM est configurée de sorte à rester ouverte jusqu'à ce que l'utilisateur la ferme explicitement. Cette stratégie RAC de l'agent Software Delivery est configurable et peut être désactivée. En cas d'échec de l'initialisation de la réinstallation hors ligne, comme en cas de méthode de téléchargement non valide ou de tentative de signalement à un serveur de modularité hérité, cet échec est signalée dans la boîte de dialogue Vérification des jobs de livraison de logiciels DSM. En outre, si le serveur de modularité n'est pas accessible, l'utilisateur final est invité à réessayer, à reporter ou à interrompre la réinstallation.

Propriétés de l'ordinateur

Le paramètre Stratégie RAC de la stratégie d'agent est remplacé par défaut par l'onglet Software Delivery de la boîte de dialogue Propriétés de l'ordinateur. Le champ Stratégie RAC est désactivé lorsque la stratégie d'agent est définie sur True et vous ne pouvez pas modifier le paramètre.

La méthode de téléchargement DTS n'est pas prise en charge pour les ordinateurs de bureau virtuels pendant la réinstallation hors ligne après un arrêt brutal. Par conséquent, cette option n'est pas affichée dans la liste déroulante Méthode de téléchargement.

Déverrouillage d'un ordinateur virtuel

Une fois que l'agent réinstalle le logiciel, il envoie une notification indiquant la fin de la réinstallation hors ligne après un arrêt brutal au serveur de modularité qui l'envoie à son tour au gestionnaire. Dès que le gestionnaire reçoit la notification, la machine virtuelle est libérée de la réinstallation hors ligne après un arrêt brutal.

Toutefois, si l'agent a réinstallé le logiciel, mais n'est pas parvenu à envoyer la notification au serveur de modularité, vous pouvez forcer le déverrouillage de la machine virtuelle. Par exemple, si l'agent ne peut pas envoyer la notification, car le serveur n'est pas disponible à ce moment-là, vous pouvez déverrouiller la machine virtuelle.

Procédez comme suit :

1. Dans l'explorateur DSM, sélectionnez Ordinateurs et utilisateurs, Tous les ordinateurs.
2. Cliquez avec le bouton droit de la souris sur l'actif approprié dans le volet Tous les ordinateurs correspondant.
3. Sélectionnez la commande Effacer le verrou de réinstallation après un arrêt brutal en attente dans le menu contextuel qui s'affiche.

   Remarque : Cette nouvelle commande est disponible uniquement si la colonne Statut SD indique qu'une ou plusieurs machines virtuelles sont verrouillées par réinstallation après un arrêt brutal. Dans le cas contraire, la commande est désactivée. En outre, elle n'est activée pour aucun ordinateur standard dont l'état est Verrouillé par réinstallation après un arrêt brutal.

   L'actif sélectionné est déverrouillé.

Suppression de la machine virtuelle de l'explorateur DSM

Si un modèle Or est déplacé d'un gestionnaire de domaines à un autre une fois que les clones sont créés, le modèle Or est déplacé selon la fonctionnalité de déplacement standard. Toutefois, si les clones créés à partir de ce modèle Or sont recomposés, ils rendent compte automatiquement au nouveau gestionnaire de domaines. Par conséquent, aucun élément ne doit être déplacé pour un clone recomposé, car tout son historique d'installation est recréé à l'aide de l'option Réinstallation hors ligne après un arrêt brutal.

Pour nettoyer les clones obsolètes qui rendaient compte au gestionnaire de domaines précédent, mais ne sont plus gérés par celui-ci, supprimez manuellement tous les clones déplacés de ce gestionnaire après la recomposition des clones du modèle Or.

Si le modèle de nommage est modifié et une machine virtuelle est supprimée à l'aide de VMWare View, une nouvelle machine virtuelle est créée avec un nouveau nom. Dans ce cas, supprimez manuellement la machine virtuelle de l'explorateur DSM.

Procédures logicielles

Le système Software Delivery vous permet actuellement d'activer ou de désactiver la réinstallation après un arrêt brutal pour les procédures logicielles individuelles. Si vous ne souhaitez pas qu'une procédure d'élément soit exécutée dans le cadre du processus de réinstallation après un arrêt brutal, sélectionnez l'option Exclure de la réinstallation après un arrêt brutal dans la boîte de dialogue Propriétés de la procédure en cours. Cette option vous permet d'exclure les packages ou les patchs obsolètes de la réinstallation après un arrêt brutal.

La fonctionnalité Exclure de la réinstallation après un arrêt brutal a été développée pour prendre en charge la réinstallation hors ligne après un arrêt brutal. Pendant la réinstallation hors ligne, le paramètre Exclure de la réinstallation après un arrêt brutal de la boîte de dialogue Propriétés est vérifié pour chaque procédure logicielle. La procédure n'est pas exécutée si elle est exclue.

Par exemple, cette option est utile lorsqu'un patch est requis pour résoudre un problème de sécurité critique impliquant vos ordinateurs de bureau virtuels, sans devoir les recomposer. Toutefois, une fois recomposée, la nouvelle version du modèle Or comprend tous les patchs appliqués et réinstaller le patch est inutile.

Application des patchs de sécurité sur les ordinateurs de bureau virtuels

Pour déclencher la réinstallation de logiciels sur les ordinateurs de bureau virtuels qui ne conservent pas les modifications une fois l'utilisateur déconnecté ou l'ordinateur redémarré, Client Automation effectue le processus de réinstallation hors ligne après un arrêt brutal. Lorsque l'utilisateur se connecte à nouveau à l'ordinateur de bureau virtuel, ce processus réinstalle les logiciels et patchs que l'utilisateur avait installés avant la déconnexion ou le redémarrage.

(Facultatif) Configuration de Patch Manager pour la gestion du déploiement de patchs lors d'une réinstallation après un arrêt brutal ou sur les ordinateurs de bureau virtuels recomposables

Par défaut, le déploiement de patchs est exclu lors d'une réinstallation après un arrêt brutal car les patchs sont redéployés sans tenir compte de l'ordre des remplacements et des transferts, ce qui peut entraîner un résultat inattendu. De même, les cibles figurant dans la liste noire sont également exclues lors du déploiement de patchs.

Par défaut, les ordinateurs de bureau virtuels recomposables font partie de cette liste noire. Les paramètres par défaut permettant d'exclure certains éléments lors d'une réinstallation après un arrêt brutal et d'ignorer les ordinateurs figurant sur la liste noire sont idéaux pour gérer le déploiement de patchs. Vous pouvez changer les paramètres pour modifier le comportement par défaut.

Procédez comme suit:

1. Connectez-vous à CA Patch Manager.
2. Sélectionnez Administration, Configuration, Paramètres du système, DSM, Options.

   Les options de configuration s'affichent.
3. Modifiez les paramètres suivants à votre convenance :

   Exclure de la réinstallation après un arrêt brutal

   Exclut le déploiement de patchs lors d'un processus de réinstallation après un arrêt brutal. Désactivez cette option pour déployer des patchs lors d'un processus de ce type. Les patchs seront redéployés sans tenir compte de l'ordre des remplacements et des transferts, ce qui peut entraîner un résultat inattendu.

   Exclure du déploiement les ordinateurs figurant dans la liste noire

   Spécifie l'option par défaut lorsque des cibles figurant sur la liste noire sont ajoutées à la liste des cibles sélectionnées lors du déploiement de patchs. Désactivez cette option pour inclure les cibles figurant sur la liste noire qui sont sélectionnées pour le déploiement de patchs. Vous pouvez également modifier cette option pour des déploiements spécifiques. Pour toujours ignorer les cibles incluses dans la liste noire sauf mention contraire, maintenez cette option activée.

   Exclure de la stratégie les ordinateurs figurant dans la liste noire

   Indique que les cibles figurant sur la liste noire doivent être ignorées pendant l'évaluation de la stratégie. L'activation de cette option ajoute la requête de liste noire CA PM aux requêtes de stratégie CA PM.

   Une requête de liste noire permet de récupérer une liste d'ordinateurs exclus du déploiement de patchs. Par défaut, le paramètre blacklistQuery est défini sur CA PM – Requête des ordinateurs inclus dans la liste noire. Cette requête est liée à une autre requête nommée Ordinateurs recomposables, qui permet de récupérer les ordinateurs de bureau recomposables basés sur un élément d'inventaire. L'élément d'inventaire IsRecomposable se trouve dans Inventaire, Système d'exploitation, Paramètres de modèle. Outre les ordinateurs de bureau recomposables, vous pouvez également inclure des ordinateurs dans la requête CA PM – Ordinateurs inclus dans la liste noire ou créer une requête pour exclure ces ordinateurs. Vérifiez que la nouvelle requête inclut la requête nommée Ordinateurs recomposables. Si vous créez une requête pour les ordinateurs inclus dans la liste noire, spécifiez le nom de la requête dans le paramètre blacklistQuery.

   Remarque : Pour mettre à jour les stratégies et packages CA PM existants de manière automatique, vérifiez que vous les avez mis à niveau. Pour plus d'informations sur la mise à niveau, reportez-vous à la rubrique sur la mise à niveau des stratégies et des packages de CA Patch Manager.
4. Enregistrez les paramètres.

Le gestionnaire de patchs est configuré pour gérer la réinstallation après un arrêt brutal (RAC) et les ordinateurs inclus dans la liste noire lors du déploiement de patchs.

Application du patch sur le vDisk ou le modèle Or

L'application des patchs de sécurité sur le vDisk ou le modèle Or garantit l'installation des patchs de sécurité requis sur tous les ordinateurs de bureau virtuels. Pour appliquer le patch sur le vDisk ou le modèle Or, suivez la procédure décrite dans le scénario Mise à jour du modèle Or.

Application du patch sur des cibles incluses dans la liste noire ou sur des ordinateurs de bureau recomposables

Par défaut, les ordinateurs de bureau recomposables font partie des cibles figurant sur la liste noire, lesquelles sont exclues du déploiement de patchs. Toutefois, vous pouvez appliquer le patch sur des cibles incluses dans la liste noire lorsque cela est nécessaire.

Procédez comme suit:

1. Connectez-vous à CA Patch Manager et cliquez sur le patch que vous voulez appliquer sur les cibles incluses dans la liste noire.
2. Dans la page Détails du patch, cliquez sur Déployer le patch.
3. Sélectionnez le groupe qui contient les cibles incluses dans la liste noire ou sélectionnez des cibles spécifiques de la liste noire et ajoutez-les au volet Cibles sélectionnées adjacent.

   La liste des cibles du groupe ou des éléments sélectionnés qui figurent sur la liste noire s’affiche dans le volet Cibles incluses dans la liste noire.
4. Dans ce volet, sélectionnez les cibles sur lesquelles vous voulez appliquer le patch. Ajoutez ces cibles au volet Cibles sélectionnées adjacent. Cliquez sur Suivant.
5. Spécifiez la planification du déploiement. Cliquez sur Suivant.
6. Désactivez l'option Exclure du déploiement les ordinateurs figurant dans la liste noire. Cliquez sur Terminer.

   Le déploiement du patch sur les cibles sélectionnées commence au moment planifié.

Affichage de l'inventaire de VDI

Les informations d'inventaire sont collectées pour le modèle Or et pour les ordinateurs de bureau virtuels avec des valeurs différentes, qui indiquent si un ordinateur de bureau virtuel est un modèle ou un clone.

Procédez comme suit:

1. Dans l'explorateur DSM, sélectionnez Ordinateurs et utilisateurs, Tous les ordinateurs, Nom de l'ordinateur, Inventaire, noeud Système d'exploitation.

   Le volet Système d'exploitation s'affiche.

2. Vérifiez la valeur de l'attribut Machine virtuelle.

   Elle indique si l'ordinateur est une machine virtuelle.

3. Sélectionnez Paramètres de modèle.

   Les informations suivantes s'affichent :

   IsGoldenTemplate

   Spécifie si une machine virtuelle est un modèle Or (True) ou un clone (False).

   Recomposable

   Spécifie si un ordinateur de bureau virtuel est recomposable.

   TemplateHostUUID

   (Clones uniquement) Spécifie l'UUID d'hôte du modèle Or.

   TemplateName

   (Clones uniquement) Spécifie le nom du modèle Or.

   TemplateTag

   (Clone uniquement) Spécifie la date et l'heure du cliché de modèle balisé.

4. Historique des modèles

   Affiche l'historique des modèles pour le clone si les clichés sont balisés.

5. Pour afficher l'inventaire de virtualisation collecté, accédez à Ordinateurs et utilisateurs, Tous les ordinateurs, Nom de l'ordinateur, Inventaire, Virtualisation.

   Affiche la technologie de virtualisation d'ordinateur de bureau que l'ordinateur utilise.

6. Développez le noeud Virtualisation et sélectionnez les éléments suivants :

   VMware View

   Affiche le nom du pool et la version de l'agent.

   Configuration de Citrix XenDesktop

   Affiche les informations relatives à la batterie de serveurs Citrix, au groupe, à la gestion des licences et au produit.

Remarque : Comme toute autre donnée d'inventaire, vous pouvez utiliser l'inventaire de virtualisation pour créer des requêtes et des rapports.

Requêtes et génération de rapports

Pour permettre la prise en charge des requêtes et de la génération de rapports sur les ordinateurs de bureau modèles, en plus des ordinateurs de bureau basés sur ces modèles, l'inventaire du matériel de base a été étendu à l'aide des attributs et des valeurs suivantes :

Is Golden Template (Modèle Or)

Booléen

Based on Template Name (Basé sur le nom du modèle)

Chaîne

Based on Template Version (Basé sur la version du modèle)

Nombre entier

Based on Template Host UUID (Basé sur l'UUID de l'hôte du modèle)

Chaîne

Ces attributs sont affichés dans le volet Tous les ordinateurs, *nom_ordinateur*, Inventaire, Système d'exploitation de l'explorateur DSM.

Modifications du concepteur de requêtes

Lors de la création d'une requête, vous disposez désormais d'arguments supplémentaires pour générer des rapports sur les ordinateurs en cours de réinstallation hors ligne après un arrêt brutal. En outre, des requêtes prédéfinies ont été ajoutées pour la prise en charge de VDI.

- Pour les requêtes basées sur un ordinateur, la valeur Hors ligne a été ajoutée à la liste déroulante Stratégie RAC dans la boîte de dialogue Sélectionner le champ du concepteur de requêtes.
- Deux requêtes de prise en charge de VDI prédéfinies, Tous les modèles Or et Tous les clones des modèles Or, ont été ajoutées au noeud Requêtes de l'explorateur DSM.

Modifications du générateur de rapports DSM

Les modèles de rapport prédéfinis suivants ont été ajoutés au générateur de rapports DSM pour la prise en charge de VDI :

- Tous les modèles Or
- Tous les clones des modèles Or

Une fois qu'un modèle de rapport est exécuté et que l'inventaire est collecté, ces rapports répertorient tous les modèles Or détectés et leurs machines virtuelles correspondantes.

Exclusion des images Or par l'assistant d'actifs obsolètes

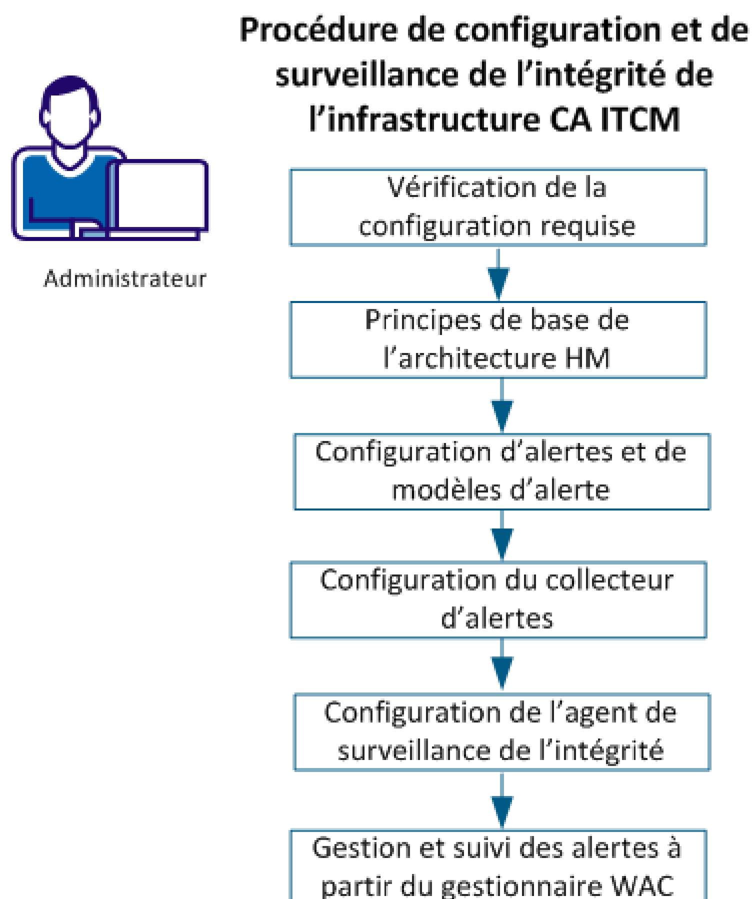
L'assistant d'actifs obsolètes vous aide à suivre les anciens ordinateurs et utilisateurs inutilisés et à les supprimer le cas échéant. Les modèles Or sont logiquement différents des ordinateurs standard et de leurs utilisateurs. Ils ont donc été exclus des ensembles de résultats des requêtes d'actifs obsolètes générées par l'assistant. Les requêtes d'actifs obsolètes créées à l'aide d'une version précédente de CA IT Client Manager n'exclut pas les modèles Or et les utilisateurs associés. Par conséquent, remplacez toutes les requêtes d'actifs obsolètes existantes pour vous assurer que les modèles Or sont exclus des ensembles de résultats.

Chapitre 9: Procédure de configuration et de surveillance de l'intégrité de l'infrastructure Client Automation

En tant qu'administrateur, il vous incombe de gérer l'intégrité des composants de Client Automation. La fonctionnalité de surveillance de l'intégrité fournit un mécanisme d'inspection d'intégrité pour :

- Définir les conditions de l'intégrité de Client Automation
- Surveiller régulièrement l'infrastructure
- Déclencher une alerte lorsqu'une condition définie est détectée.
- Informer l'administrateur par l'envoi d'un courriel, le déclenchement d'une interruption SNMP et l'écriture dans les journaux d'événements Windows/CCS.
- Configuration des actions correctrices des alertes

Utilisez la fonctionnalité de surveillance de l'intégrité pour améliorer la disponibilité et la résilience de Client Automation. L'illustration suivante résume le processus de surveillance de l'intégrité :



Vous pouvez effectuer les tâches suivantes :

Configuration des alertes

Configuration des alertes disponibles ou définition de nouvelles alertes

Configuration des actions alertes

Configuration des actions d'alerte, telles que l'envoi de courriels, le déclenchement d'interruptions SNMP, l'écriture dans le journal système et le journal d'événements CCS

Gestion des alertes

Affichage, suivi et effacement des alertes à partir de la console d'administration Web

Ce chapitre traite des sujets suivants :

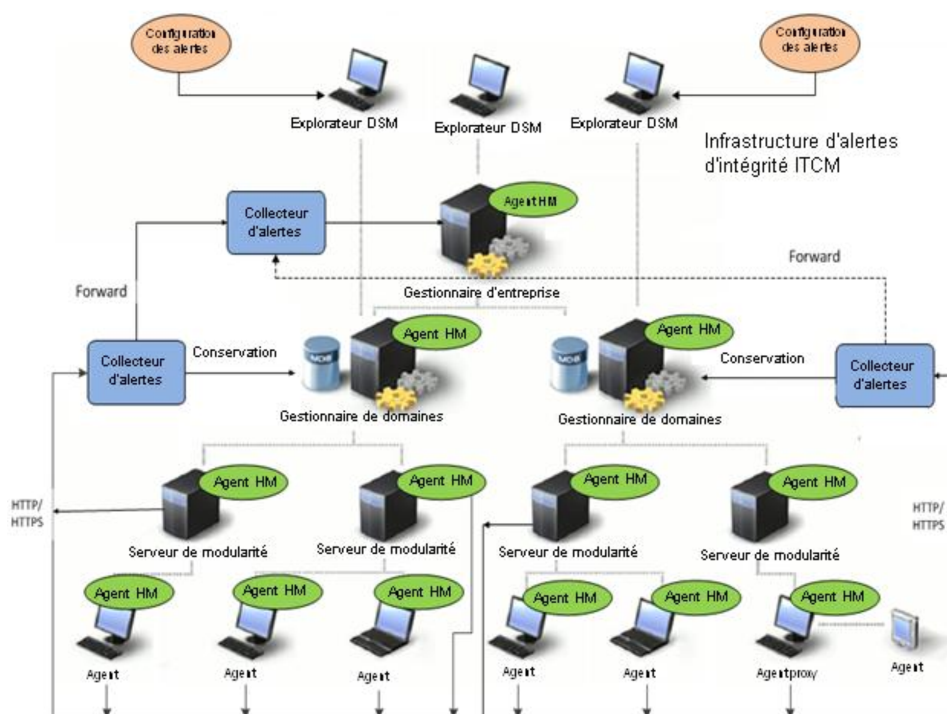
Vérification de la configuration requise

Conditions préalables à la configuration et à la surveillance des alertes de surveillance de l'intégrité :

- Connaissances suffisantes pour utiliser l'infrastructure Client Automation
- Compréhension de l'architecture de surveillance de l'intégrité et des notions de base
- Mise à niveau de l'infrastructure existante avec Client Automation Version 12.9
- Installation du collecteur d'alertes

Introduction à l'architecture de surveillance de l'intégrité et notions de base

Le diagramme suivant décrit les composants de la fonctionnalité de surveillance de l'intégrité, ainsi que leurs interactions pour surveiller l'intégrité de Client Automation :



Pour plus d'informations sur les principes de base de la surveillance de l'intégrité, consultez les rubriques suivantes :

- Alertes et modèles d'alerte (page 351)
- Composants de la surveillance d'intégrité (page 352)
- Gestionnaire de processus externes (module d'extension de CAF) (page 354)

Alertes et modèles d'alerte

La fonctionnalité de surveillance de l'intégrité permet de surveiller les types alertes suivants :

Alertes paramétrées (modèles d'alerte) :

Les alertes paramétrées prennent en charge des paramètres supplémentaires dans la définition d'alerte. Vous pouvez personnaliser les propriétés d'alerte, telles que la fréquence de la surveillance, le seuil et la sévérité selon les valeurs définies pour ces paramètres. La définition et la configuration d'alertes paramétrées sont prises en charge via les modèles d'alerte.

Les modèles d'alerte fournissent une définition par défaut d'une alerte paramétrée avec une liste de paramètres pris en charge. Utilisez le modèle comme référence pour créer une ou plusieurs alertes avec des valeurs de paramètre différentes et les configurations associées.

Alertes simples ou non paramétrées (alertes) :

Les alertes simples ne prennent pas en charge les paramètres supplémentaires. Utilisez les propriétés d'alerte telles qu'elles sont définies dans le système.

La fonctionnalité de surveillance de l'intégrité fournit des modèles d'alerte et des alertes prêts à l'emploi. Vous pouvez créer des alertes et des modèles personnalisés selon le script du gestionnaire de domaines. Pour une liste d'alertes et de modèles d'alerte, reportez-vous à l'interface utilisateur.

Composants de la surveillance d'intégrité

La fonctionnalité de surveillance de l'intégrité contient les composants suivants :

Agent HM:

Un module persistant installé avec l'agent commun qui réside sur tous les niveaux de l'infrastructure Client Automation.

- Il interprète la configuration d'alerte sur les agents, surveille régulièrement l'occurrence des conditions d'alerte et notifie l'administrateur en cas de détection des conditions d'intégrité.

  Remarque : La surveillance d'alerte est désactivée par défaut. Pour activer surveillance d'intégrité, appliquez une stratégie de configuration.

- Ce composant fournit les options de ligne de commande suivantes relatives à l'interaction :

  `hmagent start`

  Démarre l'agent de surveillance de l'intégrité.

  `hmagent stop`

  Arrête l'agent de surveillance de l'intégrité.

  `hmagent status`

  Indique si l'agent est en cours d'exécution et si la surveillance d'intégrité est activée.

- L'agent de surveillance de l'intégrité est un service sur les plates-formes Windows et un démon sur les plates-formes Linux et UNIX.

Collecteur d'alertes :

Le collecteur d'alertes comprend les modules suivants :

Module Web

Reçoit les alertes à partir de l'agent de surveillance de l'intégrité et les copie dans un dossier configuré.

Module persistant

Surveille le dossier configuré et traite les nouvelles alertes selon le rôle de collecteur d'alertes configuré. Pour plus d'informations, consultez la rubrique Configuration du collecteur d'alertes (page 366).

Les conditions préalables pour le collecteur d'alertes sont les suivantes :

- Le collecteur d'alertes est uniquement pris en charge sur Windows.
- IIS doit être installé.
- Vérifiez que les extensions ISAPI et les filtres ISAPI disponibles sous l'option Développement de l'application sont installés.
- Selon le type de base de données sur laquelle le collecteur d'alertes conserve les alertes, le client Oracle ou SQL 32 bits doit être installé.

L'application de module Web héberge les services Web de surveillance de l'intégrité sur IIS. Ce service Web est indépendant de la fonctionnalité de services Web Client Automation existante et s'exécute dans un pool d'applications distinct.

L'administrateur peut démarrer, arrêter et interroger le statut du processus de collecteur d'alertes à partir de la ligne de commande prise en charge. Le collecteur d'alertes prend en charge les options de ligne de commande similaires à l'agent de surveillance de l'intégrité.

Remarque : Lorsque vous modifiez le mode FIPS, vérifiez la valeur du paramètre associé Action de modification. Si la valeur du paramètre n'est pas Redémarrer l'ordinateur, une fois que vous avez redémarré le CAF, vous devez également redémarrer l'un des composants ci-dessous pour faire basculer tous les composants CA Client Automation sur le mode FIPS de votre choix :

Sur un ordinateur de gestionnaire ou sur un ordinateur de collecteur d'alertes autonome :

- Collecteur d'alertes
- Agent de surveillance de l'intégrité

Sur un serveur de modularité ou un ordinateur agent :

- Agent de surveillance de l'intégrité

Alertes sur la console d'administration Web :

L'explorateur DSM affiche une notification lorsque de nouvelles alertes sont déclenchées. Cette notification contient un lien hypertexte qui lance la console d'administration Web et renvoie à la page Alertes lorsque la connexion unifiée est activée pour la console d'administration Web. Si la connexion unifiée n'est pas activée, saisissez les informations d'identification appropriées pour accéder à la page Alertes.

Gestionnaire de processus externes (module d'extension de CAF)

Ce module d'extension (cfProcessManager) gère les processus externes, tels que ceux de l'agent de surveillance de l'intégrité et du collecteur d'alertes. La fonctionnalité de module d'extension est similaire à CAF, en ce que CAF gère les modules d'extension conformes à Client Automation, mais le gestionnaire de processus gère par ailleurs les processus externes qui ne sont pas des modules d'extension de CAF.

Les processus externes que cfProcessManager gère prennent en charge les propriétés de module d'extension de CAF standard, comme *Maxinstances, Maxrestarts, Restartifdied, Enabled,* et *Maxrestarttime.* Le comportement de ces propriétés est similaire à celles des modules d'extension de CAF.

Les propriétés supplémentaires suivantes sont prises en charge :

Startwithcaf

Définit le processus à démarrer lorsque CAF démarre.

Valeur par défaut : Ne démarre pas en même temps que CAF.

Stopwithcaf

Définit le processus à arrêter lorsque CAF s'arrête.

Valeur par défaut : Ne s'arrête pas en même temps que CAF.

Commandline

Indique la ligne de commande du processus.

Startcmd

Définit la commande start. Valeur par défaut: start.

Stopcmd

Définit la commande stop. Valeur par défaut : stop

Statuscmd

Définit la commande status. Valeur par défaut : status

Remarque : Redémarrez cfProcessManager lorsque vous modifiez ces paramètres.

Une nouvelle option */EXT* est désormais disponible pour les commandes CAF start et stop.

Caf start /EXT

Démarre tous les modules d'extension et les processus externes activés que le gestionnaire de processus gère.

Caf stop /EXT

Arrête tous les modules d'extension et les processus externes activés que le gestionnaire de processus gère.

La commande **Caf status cfProcessManager** indique le statut des processus externes.

Action correctrice d'alerte

Lorsqu'une condition d'alerte particulière est détectée, vous pouvez y associer une action correctrice pour résoudre le problème sur l'ordinateur. Spécifiez l'*une* des actions correctrices suivantes :

1. Actions par défaut
2. Actions basées sur un script

Configuration des alertes et des modèles d'alerte

Vous pouvez surveiller l'intégrité des composants Client Automation, tels que le gestionnaire de domaines, le gestionnaire d'entreprise, le serveur de modularité et l'agent. Créez un modèle alerte ou une alerte et spécifiez la sévérité, le seuil et la fréquence.

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, DSM, Surveillance de l'intégrité, Configuration des alertes.
2. Configurez les entités suivantes :

   Alertes

   > Configurez les paramètres d'alerte, tels que la fréquence, le seuil, la sévérité des alertes prédéfinies et créez des alertes en fonction des modèles ou d'un script de gestionnaire de domaines.

   Modèles d'alerte

   > Configurez les paramètres des modèles d'alerte prédéfinis et créez des modèles basés sur un script de gestionnaire de domaines.

Vous avez défini un modèle d'alerte ou une alerte.

Configuration des alertes

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, DSM, Surveillance de l'intégrité, Configuration des alertes, Alertes.
2. Sélectionnez Ajouter pour créer une alerte basée sur un modèle ou un script.
3. Spécifiez les valeurs appropriées pour les champs suivants :

Nom de l'alerte

Spécifie le nom de l'alerte.

Modèle

Spécifie le nom du modèle d'alerte dont l'alerte est dérivée.

Remarque : Sélectionnez un modèle dans la liste déroulante pour créer une alerte basée sur le modèle. Par exemple, Jobs d'actif non mis à jour.

Script

Spécifie le nom du script pour les alertes basées sur un script.

Paramètres

Spécifie les paramètres appropriés à l'alerte.

Remarque : Lorsque l'alerte est dérivée d'un modèle, les paramètres de modèle sont hérités du modèle. Par exemple :
`GROUPS=ComputerGroups;RequiredPercentage=MINPERCENT;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%`

Remarque : Vous pouvez spécifier des paramètres pour des alertes basées sur un script.

Message

Définit les informations liées aux alertes, qui sont évaluées lorsqu'une condition d'alerte est détectée. Ces informations évaluées sont transférées dans l'alerte déclenchée par l'agent de surveillance de l'intégrité. Par exemple :
Moins de $PERCENTAGE des ordinateurs ont signalé que le job d'actif provient du groupe d'ordinateur $GROUPS.

Severity

Configure la sévérité de l'alerte à partir de la liste déroulante.

Activer

Spécifie l'état de l'alerte. Lorsque vous définissez cette option sur True, l'alerte est surveillée par l'agent de surveillance de l'intégrité. Dans le cas contraire, elle est exclue de la surveillance.

Niveaux de détection

Spécifie les niveaux sur lesquels l'alerte est détectée. Par exemple, Gestionnaire d'entreprise, Gestionnaire de domaines, Serveur de modularité et Agent.

Remarque : Pour des alertes prédéfinies, sélectionnez le niveau dans la liste prise en charge. Pour une alerte basée sur un modèle, sélectionnez un niveau à partir des niveaux pris en charge par le modèle.

Fréquence

Spécifie la fréquence à laquelle l'alerte est surveillée. Vous pouvez spécifier une fréquence en minutes, en heures ou en jours pour chaque niveau détecté.

Seuil

Spécifie la valeur de seuil par défaut. Cette valeur indique les minutes/heures/jours qu'une condition d'alerte est présente ou le nombre de fois qu'une condition d'alerte se produit avant de déclencher une alerte.

Par exemple, lorsque vous configurez le paramètre Problème de communication de l'agent avec le serveur de modularité avec une fréquence d'une heure et un seuil de six heures au niveau de l'agent, l'agent de surveillance de l'intégrité effectue un contrôle toutes les heures pour déterminer si l'agent peut communiquer avec le serveur de modularité distant. En cas d'impossibilité de communiquer de plus de six heures, une alerte est déclenchée.

Remédiation

Identifie les méthodes d'action correctrice pour l'alerte.

hmStartCaf.dms

Redémarre le service CAF.

hmRepairWinAgent.dms

Répare les composants spécifiés sous Paramètres. Les agents doivent être stockés sur un média intermédiaire sur le serveur de modularité (applicable uniquement à Windows).

Paramètres

Spécifie le ou les composants sur lesquels l'action correctrice est requise. Par exemple, pour hmRepairAgent.dms, vous pouvez spécifier AM, SD, RC et ALL pour lesquels une réparation est requise comme action correctrice.

Remarque : Spécifiez des combinaisons d'AM, SD, RC et ALL dans une liste, séparées par des virgules.

4. (Facultatif) Cliquez sur Vérifier pour vérifier les valeurs.
5. Cliquez sur Appliquer, puis sur OK.

   Vous avez configuré une alerte.

Création d'alertes basées sur un script du gestionnaire de domaines

Vous pouvez créer des alertes personnalisées basées sur un script du gestionnaire de domaines. Déployez le script vers le répertoire de scripts configurés sous *Stratégie de configuration, DSM, Surveillance de l'intégrité, Agent, ScriptDir*, sur les agents avant d'appliquer la configuration relative à ces alertes.

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, DSM, Surveillance de l'intégrité, Configuration des alertes, Alertes**.**
2. Sélectionnez Ajouter pour créer une alerte basée sur un script et laissez le champ de nom de modèle vide.
3. Spécifiez le nom de script de gestionnaire de domaines qui est déployé vers les agents.
4. Spécifiez les paramètres dans les champs Paramètres.
5. Dans le champ Message, ajoutez un texte relatif à l'alerte (paramètres disponibles).
6. Définissez d'autres paramètres d'alerte et appliquez-les aux agents à surveiller.

Exemple d'alerte de script de gestionnaire de domaines :

Le script du gestionnaire de domaines suivant signale la présence ou l'absence de condition d'alerte à l'agent de surveillance de l'intégrité en appelant hmAlertOPFormatter. Par exemple :

```
'Ecrivez votre script de vérification d'alerte ici.
'...
' Au bas de votre script de gestionnaire de domaines, exécutez
hmAlertOPFormatter
' pour créer la sortie XML de l'alerte.
dim ret as integer
ret = Exec("hmAlertOPFormatter.exe alertconditionexist=1 raisealertnow=1
""param1=" + argv(1)  + ",param2=" + argv(2) + """ additionalinfo=this is
some additional text for script with Args", true)
print "hmAlertOPFormatter.exe: " + str(ret)
```

Pour créer un fichier XML à traiter par l'agent de surveillance de l'intégrité lorsqu'il est appelé pour des alertes de surveillance, exécutez la commande suivante dans le script du gestionnaire de domaines :

Fichier exécutable hmAlertOPFormatter

```
hmAlertOPFormatter.exe alertconditionexist=0|1 [raisealertnow=0|1]
[PARAM1=data1,PARAM2=data2,..,PARAMX=datax] [additional info=Additional Info]
```

`alertconditionexist=0|1`

Utilisez la valeur 0 lorsque votre script de gestionnaire de domaines n'a déterminé aucune condition d'alerte. Utilisez la valeur 1 lorsque votre script a déterminé une condition d'alerte.

`raisealertnow=0|1`

(Facultatif) La valeur par défaut est 0. Utilisez la valeur 1 pour déclencher l'alerte immédiatement.

`PARAM1=data1,PARAM2=data2 .. PARAMX=datax –`

(Facultatif) Ces paires de clé-valeur indiquent les paramètres et leurs valeurs dans le message d'alerte. La séquence de paires de clé-valeur est séparée par une virgule, tandis que les clés et les valeurs sont séparées par un signe égal (=).

`additionalinfo=<Additional Info>`

(Facultatif) Ce paramètre est le dernier dans la ligne de commande. Tout le reste de la ligne de commande après le signe égal (=) est cumulée comme un champ de fichier XML d'alerte résultante.

Création d'un script d'action correctrice à l'aide d'un script du gestionnaire de domaines

Vous pouvez créer des scripts d'action correctrices basées sur un script du gestionnaire de domaines. Déployez le script vers le répertoire de scripts configurés sous Stratégie de configuration, DSM, Surveillance de l'intégrité, Agent de surveillance de l'intégrité, ScriptDir, sur les agents avant de configurer les alertes à utiliser pour le script d'action correctrice.

Procédez comme suit :

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, DSM, Surveillance de l'intégrité, Configuration des alertes, Alertes.
2. Sélectionnez une alerte pour laquelle vous voulez configurer une action correctrice.
3. Sous la section d'action correctrice de l'alerte, spécifiez le nom de script de gestionnaire de domaines qui est déployé sur les agents.
4. Spécifiez les paramètres dans les champs Paramètres.
5. Dans le champ Message, ajoutez un texte relatif à l'alerte (paramètres disponibles).
6. Définissez d'autres paramètres d'alerte et appliquez-les aux agents à surveiller.

Exemple d'action correctrice de gestionnaire de domaines :

Le script du gestionnaire de domaines suivant indique si l'action correctrice a été appliquée à l'agent de surveillance de l'intégrité en appelant hmAlertOPFormatter. Par exemple :

```
dim remediationStatus as string

dim validate as string

dim remediationInfo as string

dim ret as integer

dim commandline as string

Appliquez l'action correctrice ici.

'...

Définissez la valeur de remediationStatus sur 0 ou 1. 0 indique que l'action
correctrice est appliquée et 1 qu'un échec s'est produit.

Définissez la valeur de remediationInfo sur la chaîne que vous voulez
afficher dans la console d'administration Web pour cette action correctrice.
IDS_REM_SUCCESS et le IDS_REM_FAILURE sont des ID de chaîne standard que vous
pouvez utiliser pour représenter la réussite et l'échec de l'action.

Définissez valudate sur 1 si la validation d'alerte est requise après
l'action correctrice, ou sur 0 dans le cas contraire.

' Au bas de votre script de gestionnaire de domaines, exécutez
hmAlertOPFormatter
```

```
pour indiquer à l'agent de surveillance de l'intégrité le statut de l'action correctrice.

If left(osstring, 3) = "Win" Then

    commandline = "hmAlertOPFormatter.exe"

Else

    commandline = "hmAlertOPFormatter"

Endif

commandline = commandline + “ statuscode=” + remediationStatus + “ validate= “ + validate + “ statusmsg=” + remediationInfo

ret = Exec(commandline, TRUE, 0)
```

Pour indiquer à l'agent de surveillance de l'intégrité le statut de l'action correctrice, exécutez la commande suivante dans le script du gestionnaire de domaines :
`Fichier exécutable hmAlertOPFormatter`

```
hmAlertOPFormatter.exe statuscode=0|1 validate=0|1 statusmsg=”<Any string>”
```

`stauscode=0|1`

Utilisez la valeur 0, si l'action correctrice est appliquée. Utilisez la valeur 1, si l'action correctrice échoue.

`Validate=0|1`

Utilisez la valeur 0, si aucune validation ne doit être effectuée pour vérifier si l'action correctrice a corrigé le problème. Utilisez la valeur 1 pour indiquer à l'agent de surveillance de l'intégrité d'effectuer une validation et renvoyer le message d'échec de l'action correctrice si la condition alerte existe encore après l'application de l'action correctrice.

`statusmsg`

(Facultatif) Message de chaîne représentant le statut de l'action correctrice.

Configuration de modèles d'alerte

Vous pouvez configurer les modèles d'alerte.

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, DSM, Surveillance de l'intégrité, Configuration des alertes, Modèles d'alerte**.**
2. Sélectionnez Ajouter pour créer un modèle d'alerte basé sur un script.
3. Spécifiez les valeurs appropriées pour les champs suivants :

Nom de l'alerte

Spécifie le nom du modèle.

Modèle

Configure le nom du modèle d'alerte dont l'alerte est dérivée. Reportez-vous à

Jobs d'actif non mis à jour (page 364)

L'inventaire des actifs n'a pas été mis à jour lors de la collecte à partir du serveur de modularité. (page 365)

Script

Spécifie le nom du script. Ce nom doit être identique à celui du fichier de script transféré à l'agent de surveillance de l'intégrité dans le dossier *ScriptDir.*

Paramètres

Spécifie les paramètres appropriés au modèle.

Remarque : Utilisez des paires nom-valeur séparées par un point-virgule pour spécifier plusieurs paramètres et par une virgule pour séparer plusieurs valeurs pour un paramètre. Par exemple :

```
GROUPS=Group1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%
```

Message

Définit les informations liées aux alertes, qui sont évaluées lorsqu'une condition d'alerte est détectée. Par exemple :

Moins de $PERCENTAGE des ordinateurs ont signalé que le job d'actif provient du groupe d'ordinateur $GROUPS.

Severity

Configure la sévérité pour le modèle d'alerte à partir de la liste déroulante.

Niveaux de détection

Spécifie les niveaux sur lesquels l'alerte est détectée. Par exemple, Gestionnaire d'entreprise, Gestionnaire de domaines, Serveur de modularité et Agent.

Fréquence par défaut

Indique la fréquence par défaut pour le modèle.

Seuil par défaut

Indique le seuil par défaut pour le modèle.

4. (Facultatif) Cliquez sur Vérifier pour vérifier les valeurs.
5. Cliquez sur Appliquer, puis sur OK.

   Vous avez configuré un modèle d'alerte.

Modèles d'alerte prédéfinis

Client Automation fournit les modèles d'alerte prédéfinis suivants.

Jobs d'actif non mis à jour (page 364)

L'inventaire des actifs n'a pas été mis à jour lors de la collecte à partir du serveur de modularité. (page 365)

Jobs d'actif non mis à jour

Ce modèle détecte si un pourcentage spécifié de jobs d'actif pour un ou plusieurs groupes d'ordinateurs n'est pas mis à jour et envoie une alerte.

Paramètres

Ce modèle prend en charge les paramètres suivants :

groups=<liste de groupes concernés séparés par des virgules>;

Spécifie un ou plusieurs noms de groupes d'ordinateurs séparés par des virgules.

requiredPercentage=<pourcentage_requis> ;

Spécifie le pourcentage requis des jobs identifiés dans les groupes spécifiés qui doivent être effectués correctement pour éviter le déclenchement d'une alerte.

IncludeLinkedGroupJobs=[TRUE]|[FALSE];

TRUE

Spécifie la valeur True pour inclure les jobs liés aux groupes pendant l'identification des jobs qui doivent être inclus pour vérification.

FALSE

Spécifie la valeur False pour ignorer les jobs liés aux groupes pendant l'identification des jobs qui doivent être inclus.

IncludeLinkedAssetJobs=[TRUE]|[FALSE];

TRUE

Spécifie la valeur True pour inclure les jobs liés aux actifs pendant l'identification des jobs qui doivent être inclus pour vérification.

FALSE

Spécifie la valeur False pour ignorer les jobs liés aux actifs pendant l'identification des jobs qui doivent être inclus.

Remarque : Lorsque vous ne spécifiez pas les paramètres *IncludeLinkedGroupJobs* ou *IncludeLinkedAssetJobs* dans la liste des paramètres, le comportement par défaut est d'inclure les types de lien de job respectifs.

assetJobNames=<liste de noms de jobs séparés par des virgules>

Spécifie les noms de job requis pour évaluation. Si vous ne spécifiez aucune valeur, tous les jobs d'actif pour le ou les groupes spécifiés sont pris en compte pour l'évaluation.

Remarque : Vous pouvez spécifier plusieurs noms de job séparés par des virgules dans le paramètre assetJobNames. Utilisez les caractères génériques suivants :

% (pourcentage)

Spécifie une chaîne de zéro ou plusieurs caractères. Par exemple, le titre LIKE %ordinateur% renvoie tous les titres de manuel contenant le mot *ordinateur.*

_ (trait de soulignement)

Spécifie un caractère unique. Par exemple, _*ean* renvoie tous les prénoms de quatre lettres finissant par *ean.*

Exemple de paramètres pour le modèle Jobs d'actif non mis à jour :

```
GROUPS=Groups1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;I
ncludeLinkedGroupJobs=FALSE;assetJobNames=%
```

L'inventaire des actifs n'a pas été mis à jour lors de la collecte à partir du serveur de modularité.

Ce modèle détecte si la mise à jour de l'inventaire échoue à partir d'un ou de plusieurs serveurs de modularité ou de groupes de serveurs de modularité pendant une période spécifiée et renvoie une alerte.

Paramètres

Ce modèle prend en charge les paramètres suivants :

Servers=<liste de serveurs de modularité séparés par des virgules>

Spécifie un ou plusieurs serveurs séparés par des virgules.

Remarque : Pour ce paramètre, vous devez spécifier le nom d'un serveur tel qu'il est répertorié dans l'explorateur DSM, pas le nom de domaine complet.

ServerGroups=<liste de groupes de serveurs de modularité séparés par des virgules>

Spécifie un ou plusieurs groupes de serveurs séparés par des virgules.

Remarque : Pour ce paramètre, vous devez spécifier le nom d'un groupe se trouvant sous Tous les serveurs de modularité, Explorateur DSM, et non à partir de la section Tous les ordinateurs et les utilisateurs.

Remarque : Lorsque vous ne spécifiez aucune valeur pour ces paramètres, tous les serveurs de modularité sont pris en compte pour l'évaluation.

Exemple de paramètres pour le modèle L'inventaire des actifs n'a pas été mis à jour lors de la collecte à partir du serveur de modularité **:**

```
Servers=Server1,Server2;ServerGroups=Group1,Group2
```

Configuration du collecteur d'alertes

Configurez le collecteur d'alertes dans l'un des rôles suivants :

Conserver les alertes dans la MDB

Configure le collecteur d'alertes pour conserver les alertes dans la MDB.

Conserver les alertes dans la MDB et appliquer les actions configurées

Configure le collecteur pour conserver les alertes dans la MDB et effectuer les actions configurées, telles que l'envoi de courriels, le déclenchement d'interruptions SNMP ou l'écriture dans le journal d'événements Windows/CCS.

Conserver les alertes, appliquer les actions et transférer

Configure le collecteur pour conserver les alertes dans la MDB, effectuer les actions configurées et envoyer les alertes à un autre collecteur d'alertes.

Remarque : Vous pouvez filtrer les alertes envoyées selon le niveau de sévérité ou de détection. Par exemple, vous pouvez envoyer uniquement les alertes de sévérité Elevée et Moyenne déclenchées dans le gestionnaire de domaines.

Transférer

Configure le collecteur pour envoyer les alertes à un autre collecteur d'alertes.

Remarque : Le collecteur d'alertes n'est pas pris en charge dans un environnement de cluster.

Pour plus d'informations sur les rôles de collecteur d'alertes, consultez la rubrique Installation de collecteur d'alertes. (page 170)

Définition des propriétés du collecteur d'alertes

Configurer le collecteur d'alertes implique la configuration du module Web et du processus de collecteur d'alertes.

Configuration du module Web :

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, DSM, Services Web, Surveillance de l'intégrité.
2. Spécifiez les valeurs appropriées pour les options suivantes :

   Dossier de chargement des alertes

   Spécifie un dossier sur l'ordinateur du collecteur d'alertes dans lequel les fichiers XML d'informations sur les alertes sont chargés.

   Valeur par défaut : *HMAlertUploads.* Ce dossier dépend du dossier d'installation de Client Automation.

   Lorsque vous n'utilisez pas la valeur par défaut, le compte d'utilisateur, sous lequel le module Web s'exécute, doit disposer des droits en écriture pour ce dossier.

   Remarque : Les chemins réseau pour l'emplacement de dossier ne sont pas pris en charge.

   Copier les fichiers dans le collecteur d'alertes

   Spécifiez la valeur 1 pour copier les fichiers chargés dans le dossier d'entrée du collecteur d'alertes.

   Valeur par défaut : 1

   Supprimer les fichiers après les avoir copiés dans le collecteur d'alertes

   Spécifiez la valeur 1 pour supprimer les fichiers XML d'informations sur les alertes après les avoir copiés dans le dossier d'entrée du collecteur d'alertes.

   Valeur par défaut : 0

Vous avez configuré le module Web.

Configuration du processus de collecteur d'alertes :

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Surveillance de l'intégrité, Collecteur d'alertes.
2. Spécifiez les valeurs appropriées pour les options suivantes :

   Rôle de collecteur d'alertes (géré localement)

   Spécifie le rôle sous lequel le collecteur d'alertes doit s'exécuter. Cette valeur est initialement définie pendant l'installation. Après l'installation, vous pouvez le remplacer par un rôle différent, de l'une des façons suivantes :

   - Changez le paramètre de rôle sur Géré de façon centralisé, définissez la valeur du rôle, puis appliquez-le au collecteur d'alertes.
   - Utilisez l'interface de ligne de commande *ccnfcmda* localement sur le collecteur d'alertes pour définir cette valeur et redémarrez le processus du collecteur d'alertes.

   Dossier des informations sur les alertes

   Spécifie un dossier sur l'ordinateur du collecteur d'alertes dans lequel les fichiers XML d'informations sur les alertes sont chargés.

   Valeur par défaut : AlertCollectorInput Ce dossier dépend du dossier d'installation de Client Automation.

   Lorsque vous n'utilisez pas la valeur par défaut, le compte d'utilisateur, sous lequel le module Web s'exécute, doit disposer des droits en écriture pour ce dossier.

   Remarque : Les chemins réseau pour l'emplacement de dossier ne sont pas pris en charge.

Gestionnaire (géré localement)

Configure le gestionnaire auquel le collecteur d'alertes doit se connecter. Cette valeur est initialement définie pendant l'installation. Suivez la procédure Rôle de collecteur d'alertes (géré localement) pour changer le gestionnaire après l'installation.

Dossier de sortie

Configure le dossier dans lequel les fichiers XML d'informations sur les alertes sont placés après avoir été traités par le collecteur d'alertes.

Valeur par défaut : AlertCollectorOutput Ce dossier dépend du dossier d'installation de Client Automation.

Ancienneté maximum de purge des alertes

Spécifie le nombre de jours après lesquels les alertes sont purgées.

Valeur par défaut : 60 jours.

Intervalle de purge des alertes

Spécifie l'intervalle selon lequel les alertes dépassant l'ancienneté maximum de purge des alertes sont supprimées.

Valeur par défaut : 10 jours

Vous avez défini le processus du collecteur d'alertes.

Configuration des actions alertes

Configurez les actions alertes, puis appliquez-les aux collecteurs d'alertes qui sont configurés pour effectuer les actions suivantes :

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Surveillance de l'intégrité, Collecteur d'alertes, Actions d'alertes, Configuration des actions.

   La boîte de dialogue Actions d'alertes s'affiche.

2. Sélectionnez Ajouter pour créer une action pour l'une des alertes configurées.

3. Spécifiez les valeurs appropriées pour les éléments suivants :

   Nom de l'alerte

   Définit le nom de l'alerte.

   Remarque : Vous pouvez sélectionner l'alerte dans la liste.

   Actions possibles

   Spécifiez des valeurs pour les actions suivantes, à votre convenance :

   envoi d'un courriel

   Envoie les informations sur les alertes à l'adresse électronique spécifiée dans le champ *Adresse de destination.* Lorsque l'adresse n'est pas spécifiée, le courriel est envoyé à l'adresse du destinataire, spécifiée globalement dans la configuration de la messagerie SMTP.

   Déclencher une interruption SNMP

   Déclenche des interruptions SNMP et les envoient à l'adresse IP spécifiée dans le serveur SNMP. Lorsque le serveur n'est pas spécifié, les interruptions sont déclenchées et envoyées au serveur SNMP, spécifié globalement dans Actions d'alerte.

   Ecriture dans le journal d'événements Windows

   Ecrit les informations sur les alertes dans le journal d'événements Windows.

   Ecriture dans le journal d'événements CCS

   Ecrit les informations sur les alertes dans le journal d'événements CSS.

   Adresse de destination

   Configure l'adresse électronique à laquelle vous envoyez les informations sur les alertes. Vous pouvez spécifier plusieurs adresses séparées par un point-virgule.

   SNMP Server

   Configure le serveur SNMP sur lequel les interruptions SNMP sont déclenchées.

4. Cliquez sur Appliquer, puis sur OK.

   Vous avez configuré les actions pour l'alerte.

Remarque : Vous pouvez configurer les paramètres globaux pour la messagerie SMTP et le serveur SNMP à partir de la section Actions d'alerte.

Configuration de la messagerie SMTP

Configurez la messagerie SMTP avec les détails suivants :

Adresse d'expéditeur

Spécifie l'adresse de messagerie à définir dans l'en-tête de courriel. Par exemple :

Valeur par défaut : *HealthMonitoringSystem*

Remarque : Ne laissez aucun espace dans l'adresse d'expéditeur.

Serveur de messagerie

Spécifie le nom DNS ou l'adresse IP du serveur de messagerie SMTP.

Adresse de destination

Définit l'adresse électronique du destinataire. Vous pouvez spécifier plusieurs adresses séparées par un point-virgule.

Objet

Spécifie l'objet du courriel.

Valeur par défaut : *Alerte de surveillance de l'intégrité*

Configurez le serveur SNMP avec les détails suivants :

SNMP Server

Configure le serveur SNMP sur lequel les interruptions SNMP sont déclenchées.

Spécification des détails de transfert d'alertes

Appliquez ces paramètres pour les collecteurs d'alertes configurés dans un rôle de transfert.

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Surveillance de l'intégrité, Collecteur d'alertes, Transfert d'alertes.
2. Spécifiez les valeurs appropriées pour les éléments suivants :

Adresse du collecteur d'alertes

Spécifie le nom d'hôte ou l'adresse IP du serveur du collecteur d'alertes sur lequel les alertes sont transférées.

Transfert d'alertes : niveau d'alerte détecté

Spécifie les niveaux utilisés comme filtre pendant le transfert des alertes.

Valeur par défaut : DM

Transfert d'alertes : sévérité d'alerte

Spécifie la sévérité d'alerte utilisée comme filtre pendant le transfert des alertes.

Transfert d'alertes : transfert du dossier en attente

Spécifie le dossier dans lequel les fichiers XML d'informations sur les alertes renvoyant un échec lors de leur premier transfert sont placés.

Transfert d'alertes : transfert du dossier rejeté

Spécifie le dossier dans lequel les fichiers XML d'informations sur les alertes qui ne sont plus transférés sont placés.

Intervalle de récupération

Spécifie le délai en minutes pour transférer à nouveau les alertes en attente.

Utiliser le protocole HTTPS

Spécifie l'utilisation du protocole HTTPS ou HTTP pour la connexion au serveur. Lorsque cette option est définie sur True, le protocole HTTPS est utilisé. Pour configurer le collecteur d'alertes de sorte qu'il puisse se connecter via HTTPS, consultez la rubrique Configuration des paramètres de chargement des alertes (page 377).

Vous avez configuré les détails de transfert d'alertes.

Transférer les paramètres du collecteur

Configure les détails d'authentification utilisés pour la connexion et l'authentification du serveur de collecteur d'alertes auquel les alertes sont transférées.

Pour plus d'informations, consultez la rubrique Configuration des paramètres du serveur du collecteur d'alertes (page 378).

Paramètres du serveur proxy

Configure les détails du serveur proxy qui sont utilisés pour la connexion au serveur du collecteur d'alertes pour le transfert d'alertes.

Pour plus d'informations, consultez la rubrique Configurer les paramètres du proxy (page 379).

Configuration d'agent de surveillance de l'intégrité

Modifiez les propriétés de l'agent de surveillance de l'intégrité.

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Surveillance de l'intégrité, Agent de surveillance de l'intégrité.
2. Dans la boîte de dialogue Définition des propriétés, spécifiez des valeurs appropriées pour les éléments suivants :

Activer la surveillance de l'intégrité

Spécifie l'état de la surveillance de l'intégrité. Valeur par défaut : False

True

Active la surveillance de l'intégrité.

False

Désactive la surveillance de l'intégrité.

Répertoire des scripts

Spécifie le dossier dans lequel les scripts d'alerte personnalisés doivent être copiés. Valeur par défaut : scriptdir

Remarque : Lorsqu'un chemin d'accès absolu est spécifié, le dossier dépend du dossier de surveillance de l'intégrité sous le répertoire d'installation de DSM. Les chemins réseau ne sont pas pris en charge.

Répertoire de sortie des scripts

Définit le nom du dossier dans lequel la sortie des scripts d'alerte personnalisés est copiée. Valeur par défaut : scriptoutputdir

Remarque : Lorsqu'un chemin d'accès absolu est spécifié, le dossier dépend du dossier de surveillance de l'intégrité sous le répertoire d'installation de DSM. Les chemins réseau ne sont pas pris en charge.

Temporisation de script

Définit le délai en secondes que l'agent de surveillance de l'intégrité attend la fin de l'exécution du script. Valeur par défaut : 120 secondes

Remarque : Lorsque l'exécution du script échoue avec une erreur de délai d'expiration, augmentez le délai en secondes, puis réessayez.

Maximum de nouvelles tentatives de chargement

Définit le nombre de nouvelles tentatives de chargement des informations sur les alertes. Valeur par défaut : 3

Intervalle entre chaque nouvelle tentative de chargement

Définit l'intervalle en secondes après lequel le chargement des informations sur les alertes est tenté à nouveau. Valeur par défaut : 5 secondes

Activer l'action correctrice de l'alerte

Spécifie l'état de l'action correctrice de l'alerte. Valeur par défaut : False

True

Active l'action correctrice d'alerte.

False

Désactive l'action correctrice d'alerte.

Nom d'utilisateur

Spécifie l'utilisateur disposant des autorisations pour accéder à la bibliothèque de packages partagée.

Partage de la bibliothèque de packages

Spécifie l'emplacement de la bibliothèque de packages partagée. La bibliothèque doit se trouver sur un emplacement partagé.

Remarque : Lorsqu'un chemin d'accès absolu est spécifié, le dossier dépend du dossier de surveillance de l'intégrité sous le répertoire d'installation de DSM.

Délai du script d'action correctrice

Définit le délai en secondes que l'agent de surveillance de l'intégrité attend la fin de l'exécution du script d'action correctrice. Valeur par défaut : 120 secondes

Remarque : Lorsque l'exécution du script échoue avec une erreur de délai d'expiration, augmentez le délai en secondes, puis réessayez.

Mot de passe

Spécifie le mot de passe pour accéder à la bibliothèque de packages partagée.

3. Cliquez sur OK.

Vous avez activé l'agent de surveillance de l'intégrité.

Vous devez également configurer des paramètres supplémentaires pour la journalisation d'événements de surveillance de l'intégrité.

Procédez comme suit:

1. Accédez à Stratégie de configuration, Stratégie par défaut de l'ordinateur, DSM, Composants communs, Journalisation d'événements, Evénements de surveillance de l'intégrité.
2. Configurez les paramètres suivants :

   Journal des événements : Dossier de destination

   Définit l'emplacement de dossier relatif au dossier d'installation de DSM pour les fichiers de journal d'événements. Le dossier doit exister sur l'agent.

   Valeur par défaut : HM

   Journal des événements : Nom du fichier

   Définit le nom de fichier à utiliser pour journaliser les événements de surveillance d'intégrité.

   Valeur par défaut : hmevents_list.xml

Configuration des paramètres de chargement des alertes

Configurez les détails du serveur du collecteur d'alertes et appliquez-les à l'agent de surveillance de l'intégrité pour lui permettre de charger les alertes détectées.

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Services Web, Client, Surveillance de l'intégrité.
2. Spécifiez les valeurs appropriées pour les options suivantes :

   Adresse du collecteur d'alertes

   Spécifie le nom d'hôte ou l'adresse IP du serveur du collecteur d'alertes sur lequel les alertes sont chargées.

   Remarque : Pour l'agent de surveillance de l'intégrité sur le gestionnaire d'entreprise, configurez le collecteur d'alertes installé sur le gestionnaire de domaines.

   Utiliser le protocole HTTPS

   Spécifie la connexion au serveur de collecteur d'alertes via HTTP ou HTTPS.

   Valeur par défaut : la valeur False indique le protocole HTTP.

   Lorsque le collecteur d'alertes est configuré pour utiliser une connexion HTTPS, procédez comme suit sur l'agent :

   - Exportez certificat racine de l'autorité de certification au format DER à partir du serveur Web (collecteur d'alertes).
   - Copiez le certificat sur l'agent et importez-le à l'aide de la commande suivante :

```
cacertutil import -i:<chemin_accès_fichier_certificat> -it:X509V3 -trust
```

Lorsque l'agent de surveillance de l'intégrité doit se connecter au collecteur d'alertes via le proxy et le serveur de collecteur d'alertes est configuré pour authentifier les demandes du client, configurez les options suivantes :

Configuration des paramètres du serveur du collecteur d'alertes

Configurez les paramètres du serveur du collecteur d'alertes de la façon suivante :

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Services Web, Client, Surveillance de l'intégrité, Paramètres du serveur du collecteur d'alertes.
2. Spécifiez les valeurs appropriées pour les éléments suivants :

   Méthode d'authentification

   Définit la valeur qui détermine la méthode d'authentification.

   Type d'authentification HTTP

   Définit la valeur qui détermine le type d'authentification HTTP.

   Remarque : Le protocole HTTP offre les modes d'authentification De base, Résumé et NTLM.

   Domain

   Indique le nom de domaine du serveur.

   Mot de passe

   Définit le mot de passe à authentifier auprès du proxy.

   Nom d'utilisateur

   Définit le nom d'utilisateur à authentifier auprès du proxy.

Vous avez configuré les paramètres du serveur du collecteur d'alertes.

Configurer les paramètres du proxy

Configurez les paramètres de proxy de la façon suivante :

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Services Web, Client, Surveillance de l'intégrité, Paramètres du serveur proxy.
2. Spécifiez les valeurs appropriées pour les éléments suivants :

   Mot de passe du proxy

   Définit le mot de passe à authentifier auprès du proxy.

   Utilisateur du proxy

   Définit l'utilisateur à authentifier auprès du serveur.

   Adresse du serveur proxy

   Définit l'adresse du serveur proxy.

   Port du serveur proxy

   Définit le port sur lequel le proxy vérifie les demandes de connexion.

   Type de proxy

   Définit la valeur qui détermine le type de proxy. La valeur *Aucun* indique la connexion HTTP directe.

Vous avez configuré les paramètres de proxy.

Remarque : L'agent de surveillance de l'intégrité prend uniquement en charge les proxys HTTP. La prise en charge de proxy SOCKS n'est pas disponible dans cette version.

Gestion et suivi du statut des alertes à partir de la console d'administration Web

Affichage des alertes

Lorsqu'une nouvelle alerte est déclenchée, une notification s'affiche dans le portlet de statut du système du noeud de domaine dans l'explorateur DSM. Cette notification contient un lien hypertexte qui lance la console d'administration Web et renvoie l'utilisateur à la page Alertes lorsque la connexion unifiée est activée. Outre le lien hypertexte, le nombre d'alertes nouvellement déclenchées est affiché. Le nombre correspond à la somme des alertes dont l'état est Nouveau et Echec de l'action correctrice.

Pour configurer la connexion unifiée pour la console d'administration Web :

Procédez comme suit:

1. Accédez au fichier Config.properties de la console d'administration Web : INF\classes\com\ca\wac\config\ de DSM\Web Console\webapps\wac\WEB.
2. Définissez la valeur de attemptUnifiedLogin sur **True**.
3. Redémarrez Tomcat.

   ```
   Caf stop tomcat
   ```

   ```
   Caf start tomcat
   ```

La connexion unifiée pour la console d'administration Web est configurée.

Vous pouvez configurer le lien de la console d'administration Web pour l'affichage des alertes.

Procédez comme suit:

1. Ouvrez le Panneau de configuration, puis cliquez sur Configuration, Stratégie de configuration, Nom de la stratégie, DSM, Surveillance de l'intégrité, Affichage des alertes, Console d'administration Web.
2. Configurez le lien vers la page d'alertes de la console d'administration Web.

   Valeur par défaut : http://localhost/wac?context_launch_class=DSMHMAlert

   Remarque : Remplacez *localhost* par le nom d'hôte de l'ordinateur de la console d'administration Web.

Gestion et suivi du statut des alertes à partir de la console d'administration Web

Gérez les alertes à partir de la console d'administration Web en ajoutant des remarques et en mettant à jour leur état sur Nouveau, Suivi ou Effacé.

Procédez comme suit:

1. Accédez à Alertes.

   La page Alertes s'affiche.

2. Sélectionnez une ou plusieurs alertes, puis Mettre à jour ou Supprimer.

   La boîte de dialogue s'ouvre.

   - Pour effectuer une mise à jour, changez le statut des alertes à partir du menu déroulant :

     nouveau

       Spécifie une nouvelle alerte.

     Suivi

       Spécifie l'alerte à suivre.

     Effacé

       Spécifie l'état de l'alerte comme effacé.

   - Pour supprimer des alertes, sélectionnez les alertes et confirmez la suppression.

     Remarque : Vous pouvez sélectionner l'option Tout supprimer pour supprimer toutes les alertes.

3. Mettez à jour les notes avec des informations utiles pour suivre le statut de l'alerte.

4. Affichez les détails de l'action correctrice d'alerte, tels que le statut de l'action correctrice, le script de l'action correctrice, les paramètres de script d'action correctrice.

Les alertes sont mises à jour ou supprimées.

Remarque : Vous pouvez suivre, mettre à jour et supprimer les alertes à partir du niveau du gestionnaire de domaines uniquement. Toutes les alertes de surveillance de l'intégrité sur le gestionnaire d'entreprise sont en lecture seule.

Réplication d'alerte

La réplication d'alerte permet de répliquer des alertes.

- Lorsque les mises à jour des alertes dans le gestionnaire de domaines sont répliquées dans le gestionnaire d'entreprise par le moteur, aucune nouvelle alerte n'est créée lors de la réplication. Les alertes sont créées au niveau du gestionnaire d'entreprise uniquement via le transfert d'alerte au niveau du gestionnaire de domaines à l'aide de filtres appropriés.
- Avant que le moteur réplique une alerte dans le gestionnaire d'entreprise, il vérifie si l'alerte existe déjà. Lorsque l'alerte est introuvable, le moteur ne réplique pas l'alerte au niveau supérieur. Lorsqu'une alerte est supprimée au niveau du gestionnaire de domaines, l'alerte correspondante est supprimée dans le gestionnaire d'entreprise.
- Lorsqu'un gestionnaire de domaines est dissocié d'un gestionnaire d'entreprise, le paramètre de politique de configuration géré suivant vérifie si toutes les alertes comprenant l'objet domain_uuid de ce gestionnaire de domaines sont conservées au niveau du gestionnaire d'entreprise ou supprimées. Si elles sont supprimées, le moteur ne re-réplique pas les alertes du gestionnaire de domaines vers le gestionnaire d'entreprise. Ce comportement est une restriction qui intervient lorsque le gestionnaire de domaines est lié à nouveau au gestionnaire d'entreprise.

Pour modifier le paramètre qui contrôle la suppression des alertes d'un domaine particulier lors de l'annulation du lien existant entre le domaine et le gestionnaire d'entreprise, ouvrez le Panneau de configuration et accédez à Configuration, Stratégie de configuration, Stratégie par défaut de l'ordinateur, DSM, Gestionnaire, Moteurs, Supprimer les alertes répliquées lors de la suppression du lien. Définissez ensuite la valeur sur True et, lors de la suppression du lien au gestionnaire de domaines, les alertes répliquées à partir du gestionnaire de domaines seront supprimées du gestionnaire d'entreprise.

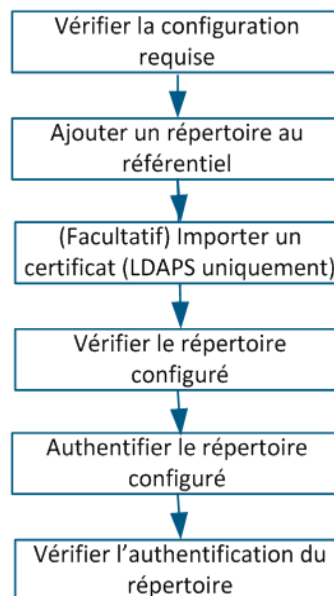
Chapitre 10: Procédure de configuration et d'authentification à l'aide d'annuaires externes

En tant qu'analyste du support informatique, vous utilisez des annuaires externes pour l'*authentification.* Utiliser des annuaires externes dans l'explorateur DSM vous permet d'effectuer les tâches suivantes :

- Authentifier les utilisateurs, y compris les utilisateurs Active Directory en mode natif
- Autoriser les utilisateurs en mappant des profils de sécurité avec des entités dans l'annuaire
- Définir des groupes de requêtes avec des cibles correspondant à des ordinateurs ou à des utilisateurs conservés dans un conteneur dans un annuaire
- Cibler le déploiement des agents
- Générer des rapports à l'aide d'une hiérarchie d'annuaire

Pour permettre l'authentification à l'aide d'annuaires externes, effectuez les opérations suivantes :





Procédez comme suit.

1. Ajout d'un annuaire au référentiel (page 384)
2. (Facultatif) Importation d'un certificat (LDAPS uniquement) (page 390)
3. Vérification de l'annuaire configuré (page 391)
4. Authentification de l'annuaire configuré (page 394)
5. Vérification de l'authentification de l'annuaire (page 397)

Annuaires externes pris en charge

Client Automation prend en charge les annuaires suivants :

- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory

Pour une liste actualisée des services d'intégration d'annuaire pris en charge, consultez la matrice de compatibilité.

Vérification de la configuration requise

Pour permettre l'authentification à l'aide d'un annuaire externe, vérifiez la configuration requise suivante :

- Vérifiez que vous disposez des droits d'accès pour la configuration d'un annuaire externe.
- Assurez-vous d'avoir les connaissances suffisantes pout utiliser la fonctionnalité d'intégration d'annuaire.

Ajout d'un annuaire au référentiel

Pour authentifier et autoriser des utilisateurs en mappant des profils de sécurité à des entités de l'annuaire, ajoutez d'abord l'annuaire externe au référentiel.

Procédez comme suit:

1. Cliquez sur Panneau de configuration, Intégration d'annuaire, Ajouter un annuaire pour accéder à l'assistant d'ajout d'annuaire.

   La page Introduction/Nom de répertoire apparaît.

2. Spécifiez le nom de l'annuaire pour l'identifier lors de la connexion à Active Directory dans le champ Nom de répertoire.

3. Sélectionnez le type d'annuaire à l'aide de l'une des options de type d'annuaire. Les options suivantes sont disponibles :

   - Active Directory
   - LDAP

   Valeur par défaut : Active Directory.

4. Cliquez sur Suivant pour accéder à la page Détails du serveur.

Spécification des détails du serveur d'annuaire

Utilisez la page de l'assistant Détails du serveur pour spécifier le nom du serveur d'annuaire contenant l'annuaire que vous ajoutez et le numéro du port auquel vous vous connectez.

Remarque : Pour les répertoires externes utilisant le protocole SSL (Secure Sockets Layer), le certificat que le serveur LDAP (Lightweight Directory Access Protocol) utilise doit être valide et vérifiable via la chaîne d'autorité de certificat Microsoft Windows. Les précédentes versions de Windows ont donné au développeur LDAP l'occasion de vérifier les certificats ; toutefois, le protocole SSL de Windows 2003 applique cela pour vous.

Procédez comme suit:

1. Dans le champ Nom du serveur, saisissez le nom du serveur prenant en charge le répertoire.
2. Dans le champ Port, entrez le numéro de port du service de répertoire.

   Le client du répertoire tente toujours de créer une connexion chiffrée sécurisée au répertoire à l'aide du port spécifié ici. Certains répertoires prennent en charge le port 389 pour les communications sécurisées et non sécurisées. Certains répertoires prennent également en charge le port 636 comme un canal sécurisé uniquement. L'administrateur de votre répertoire peut vous indiquer quel port utiliser.

   Pour le port spécifié, un canal sécurisé disponible est utilisé. Si aucun canal sécurisé n'est disponible et si le port spécifié permet une communication non sécurisée, ce port est utilisé (si une communication non sécurisée n'est pas acceptable, l'importation de répertoires est rejetée avec un message d'erreur correspondant lorsque vous cliquez sur Terminer).

   Remarque : Des stratégies de configuration communes pour les répertoires (notamment la stratégie Activer l'authentification simple LDAP) peuvent avoir un impact sur la possibilité d'occurrence de l'authentification sur un canal de communication non sécurisé.
3. Cliquez sur Suivant pour accéder à la page Liaison de répertoire.

Remarque : Si, après l'ajout d'un annuaire LDAP, le port d'accès spécifié a changé, l'autorité de sécurité *originale* n'est pas supprimée correctement et la liste des autorités de sécurité peut contenir une autorité de sécurité non valide. Cela n'a aucune conséquence fonctionnelle sur Client Automation, mais l'autorité de sécurité originale est répertoriée comme valide dans les boîtes de dialogue de sécurité. La suppression de l'autorité de sécurité extérieure nécessite un outil fourni par le support technique. Contactez votre responsable technique et demandez l'utilitaire *cfspsetpass*.

Spécification des informations de liaison d'annuaire

Utilisez la page de l'assistant Liaison de répertoire pour spécifier si vous voulez accéder au répertoire de façon anonyme ou utiliser les informations d'identification de l'utilisateur.

Procédez comme suit:

1. (Facultatif) Sélectionnez l'option Utiliser la liaison anonyme. Par défaut, cette option n'est pas activée (False).

   Remarque : Si cette option est activée, vous avez un accès limité au répertoire ou pas d'accès du tout.

2. Entrez un nom et un mot de passe utilisateur dans les champs appropriés.
3. (Facultatif) Sélectionnez l'option Utiliser un protocole sécurisé (LDAPS). Si vous sélectionnez cette option, le protocole LDAPS sécurisé est utilisé à la place de LDAP. Toutefois, assurez-vous d'abord que LDAPS est pris en charge par l'annuaire que vous configurez.

   Remarque : Ce champ apparaît uniquement si vous configurez un répertoire actif ou un répertoire LDAP.

4. Cliquez sur Suivant pour accéder à la page Noeud du répertoire de base.

Spécification des détails du noeud du répertoire de base

Utilisez la page de l'assistant Noeud du répertoire de base pour spécifier le noeud racine à partir duquel commence la navigation dans les répertoires.

Procédez comme suit:

1. Dans le champ Noeud du répertoire de base, entrez le nom unique (DN) de l'objet racine pour accéder au répertoire actuel.

   Remarque : Essayez d'utiliser un nom unique de base le plus bas possible dans la hiérarchie des répertoires, afin de garantir des recherches plus efficaces. L'administrateur de votre répertoire peut vous indiquer la meilleure valeur à utiliser.

2. Cliquez sur Suivant pour accéder à la page Choisir le mappage de schéma.

Sélection des attributs de mappage de schémas

Utilisez la page de l'assistant Choisir le mappage de schémas pour spécifier le mappage de schémas pour votre répertoire. Vous pouvez sélectionner un mappage de schéma prédéfini, commun ou le définir.

Procédez comme suit:

1. (Facultatif) Sélectionnez l'option Définir un nouveau mappage si vous souhaitez utiliser votre propre mappage de schéma.

   Cette option vous permet de définir un mappage entre les noms d'attributs associés aux objets de données (tels que les utilisateurs, les ordinateurs et les groupes) utilisés dans votre répertoire externe et les noms d'attributs utilisés par les objets DSM correspondants.

2. Sélectionnez un mappage de schéma prédéfini à l'aide de l'une des options de mappage de schéma. Les options valides sont Active Directory et eTrust.

   Valeur par défaut : Active Directory.

3. Cliquez sur Suivant pour accéder à la page Affiner/Définir le mappage de schéma.

Optimisation/définition des détails du mappage de schémas

L'assistant d'optimisation/de définition de mappage de schémas vous permet de définir un nouveau mappage de schémas ou d'optimiser le schéma spécifié. Le schéma du répertoire définit le nom et le type des attributs. Le mappage de schémas convertit les attributs ou les propriétés d'un objet de répertoire, comme défini par ce schéma de répertoire, en un schéma commun utilisé par d'autres applications basées sur DSM.

Remarque : Un certain nombre de mappages de schémas prédéfinis sont fournis pour les schémas les plus couramment utilisés, notamment les mappages préprogrammés pour les fournisseurs WinNT et UnixL.

Procédez comme suit:

1. Lors de la création d'un schéma, entrez un nom unique pour le mappage de schéma dans le champ Nom du schéma. Sinon, ce champ affiche le nom du schéma existant sélectionné.

   La table de mappage appropriée affiche le nom et le type des attributs dans le schéma d'annuaire répertoire spécifié.

2. (Facultatif) Pour modifier la valeur par défaut d'un attribut DSM, cliquez sur cet attribut dans la table de mappage.

   La boîte de dialogue Mappage d'attribut s'affiche.

3. (Facultatif) Modifiez la valeur d'un ou de plusieurs attributs DSM, puis cliquez sur OK.

   La boîte de dialogue Mappage d'attribut se ferme et vous revenez à la page de l'assistant.

4. Cliquez sur Suivant pour accéder à la page Terminer.

Pour plus d'informations sur les schémas, consultez la rubrique Mappage de schémas (page 399).

Vérification des options de configuration et ajout du répertoire

La page de l'assistant de fin résume les paramètres de configuration et les options sélectionnés pour le répertoire. Cliquez sur Terminer pour finir l'ajout de l'annuaire spécifié au référentiel ou cliquez sur Précédent pour modifier l'un des paramètres ou l'une des options.

L'annuaire externe est configuré.

(Facultatif) Importation d'un certificat (LDAPS uniquement)

Lorsque vous utilisez LDAPS pour sécuriser l'accès à un répertoire LDAP ou OpenLDAP défini, le serveur Windows doit pouvoir faire confiance au certificat du serveur LDAPS. Si le certificat ne provient pas d'une autorité de certification approuvée, vous devez alors importer manuellement le certificat dans le magasin de certificats pour terminer le processus de configuration de votre nouveau répertoire.

Remarque : Pour des informations détaillées sur les assistants et les boîtes de dialogue mentionnés dans la procédure ci-après, reportez-vous à la documentation Microsoft sur les certificats x.509.

Procédez comme suit:

1. Localisez le fichier \CA\DSM\bin\itrm_dsm_r11_root.der et double-cliquez dessus.

   La boîte de dialogue Importation du certificat s'affiche.

2. Cliquez sur Installer le certificat.

   L'assistant d'importation de certificat apparaît.

3. Cliquez sur Suivant.

   La page de l'assistant Magasin de certificats apparaît.

4. Sélectionnez l'option Placer tous les certificats dans le magasin suivant.
5. Cliquez sur Parcourir.

   La boîte de dialogue Sélection du magasin de certificats.

6. Sélectionnez l'option Afficher les magasins physiques.
7. Effectuez l'*une* des opérations suivantes :
   - Si le certificat est auto-signé, développez Autorités de certification racine de confiance et sélectionnez Ordinateur local.
   - Si le certificat n'est *pas* auto-signé, développez Autorités de certification racine tierce partie et sélectionnez Ordinateur local.

   Important : Cette étape est essentielle. Le certificat doit être ajouté au magasin physique. Sinon, le magasin de l'utilisateur actuel sera utilisé et le certificat ne sera pas disponible pour le compte système local utilisé par Client Automation.

8. Cliquez sur OK.

   La boîte de dialogue se ferme et vous revenez à l'assistant.

9. Cliquez sur Suivant, puis sur Terminer.

   Le message informant de la fin de l'importation s'affiche.

10. Cliquez sur OK.

    Le certificat spécifié a été ajouté au magasin de certificats.

Remarque : Vous pouvez également utiliser la commande encUtilCmd certimport pour effectuer la même opération.

Vérification de l'annuaire configuré

Après avoir ajouté et configuré l'annuaire, vous pouvez vérifier s'il a été ajouté à l'explorateur DSM.

Procédez comme suit:

1. Accédez à Panneau de configuration, Intégration d'annuaire, Répertoires configurés.

   Le nom et la description de tous les *annuaires externes* configurés dans le domaine actuel sont affichés. La colonne de description affiche une URL LDAP pour chaque annuaire Active Directory configuré, le cas échéant.

L'annuaire externe est configuré.

(Facultatif) Mise à jour de l'annuaire

Vous pouvez également mettre à jour les propriétés de l'annuaire.

1. (Facultatif) Mise à jour d'un annuaire configuré à l'aide de ses propriétés.

   La boîte de dialogue Mettre à jour un répertoire avec les onglets suivants s'affiche.

   - Paramètres (page 392)
   - Sécurité
   - Schéma (page 394)

Mise à jour du répertoire : onglet Paramètres

L'onglet Paramètres permet de modifier les principales options de configuration des répertoires.

Cet onglet contient les champs suivants :

Nom du répertoire

Spécifie l'annuaire ou le nom de serveur d'annuaire comme suit :

- Spécifie le nom utilisé pour identifier le répertoire lors de la connexion à Active Directory. Cette valeur doit être un nom que le répertoire lui-même peut reconnaître comme un serveur de répertoires.
- Spécifie le nom du serveur de répertoires lors de la connexion à un répertoire autonome (c'est-à-dire un répertoire qui n'est pas distribué comme Active Directory) à l'aide de LDAP. Le nom doit être le nom DNS complet du serveur qui sera utilisé pour l'autorisation et l'accès au répertoire.

Exemple : Un domaine Active Directory HQDirectory.com est hébergé sur l'ordinateur FAKE_MACHINE. Lors de la configuration de ce répertoire pour l'intégration, vous pouvez spécifier HQDirectory.com dans ce champ, comme Active Directory peut reconnaître HQDirectory.com sur FAKE_MACHINE.

Type d'annuaire

Spécifie le type d'annuaire. Les options valides sont Active Directory et LDAP. Le type de répertoire spécifié lors de l'ajout du répertoire est sélectionné par défaut.

Serveur d'annuaire

Spécifie le nom du serveur prenant en charge l'annuaire.

Port

Spécifie le numéro de port du service d'annuaire. Le client du répertoire tente toujours de créer une connexion chiffrée sécurisée au répertoire à l'aide du port spécifié ici. Certains répertoires prennent en charge le port 389 pour les communications sécurisées et non sécurisées. Certains répertoires prennent également en charge le port 636 comme un canal sécurisé uniquement. L'administrateur de votre répertoire peut vous indiquer quel port utiliser.

Pour le port spécifié, un canal sécurisé disponible est utilisé. Si aucun canal sécurisé n'est disponible et si le port spécifié permet une communication non sécurisée, ce port est utilisé (si une communication non sécurisée n'est pas acceptable, l'importation de répertoires est rejetée avec un message d'erreur correspondant lorsque vous cliquez sur Terminer).

Remarque : Des stratégies de configuration communes pour les répertoires (notamment la stratégie Activer l'authentification simple LDAP) peuvent avoir un impact sur la possibilité d'occurrence de l'authentification sur un canal de communication non sécurisé. Pour plus d'informations, reportez-vous à la section Stratégie de configuration de *l'aide de l'explorateur DSM*.

Valeur par défaut : 389 (pour les répertoires LDAP)

DN de base

Spécifie le nom unique de l'objet racine pour parcourir le répertoire actuel. Contactez l'administrateur de votre répertoire pour connaître la meilleure valeur à utiliser.

Remarque : De nombreuses recherches de répertoires pouvant être effectuées depuis ce noeud racine, réfléchissez attentivement à l'efficacité et à la précision des recherches effectuées. Essayez d'utiliser un DN de base aussi bas que possible dans la hiérarchie des répertoires : cela garantira des recherches plus efficaces.

Informations

Affiche des conseils relatifs à la sélection d'options ou à la saisie d'informations dans les champs ou les boîtes de dialogue.

Mise à jour du répertoire : onglet Sécurité

L'onglet Sécurité fournit les options de sécurité pour la connexion au répertoire.

Cet onglet contient les champs suivants :

Liaison anonyme

Indique si la liaison anonyme doit être utilisée. La valeur spécifiée lors de l'ajout du répertoire est sélectionnée par défaut.

Utilisateur

Spécifie le nom de l'utilisateur si Liaison anonyme n'est pas sélectionnée.

Mot de passe

Spécifie le mot de passe de l'utilisateur spécifié si Liaison anonyme n'est pas sélectionnée.

Informations

Affiche des conseils relatifs à la sélection d'options ou à la saisie d'informations dans les champs ou les boîtes de dialogue.

Mise à jour du répertoire : onglet Schéma

L'onglet Schéma contient les options de configuration qui permettent de mapper des attributs de répertoire vers le schéma Client Automation.

Cet onglet contient les champs suivants :

Schéma

Indique le schéma à utiliser. Un certain nombre de mappages de schémas prédéfinis sont fournis pour les schémas les plus couramment utilisés, notamment les mappages préprogrammés pour les fournisseurs WinNT et UnixL. Sélectionnez un schéma dans la liste déroulante.

Informations

Affiche des conseils relatifs à la sélection d'options ou à la saisie d'informations dans les champs ou les boîtes de dialogue.

Authentification à l'aide du répertoire configuré

L'authentification identifie les membres d'une base informatique sécurisée, basée sur les informations d'identification fournies. Ajoutez les annuaires externes en tant qu'autorité de sécurité pour des opérations d'autorisation de DSM. Client Automation authentifie un objet de sécurité auprès du répertoire externe et utilise l'identité authentifiée ou les appartenances aux groupes pour les appels d'autorisation suivants.

Ajout d'un profil de sécurité

La création d'un profil de sécurité signifie en mapper un nouveau sur un compte utilisateur ou un groupe proposé par les fournisseurs de sécurité actuels. Vous pouvez sélectionner les utilisateurs ou les groupes qui peuvent accéder au système et les ajouter à un profil de sécurité.

Procédez comme suit:

1. Sélectionnez des profils de sécurité à partir du menu Sécurité.

   La boîte de dialogue Profils de sécurité s'affiche.

   Remarque : Vous devez disposer des droits d'accès permettant d'ouvrir cette boîte de dialogue ; sinon, un message d'erreur de sécurité apparaît. Les administrateurs disposent de ces droits d'accès par défaut.

2. Cliquez sur Ajouter.

   La boîte de dialogue Ajouter des profils de sécurité apparaît.

3. Sélectionnez l'autorité de sécurité à partir de l'arborescence des répertoires disponibles, parcourez et cliquez sur l'entité de sécurité requise.

   Vous pouvez afficher l'autorité et l'entité de sécurité sélectionnées respectivement dans l'identificateur de conteneur et les champs Noms.

4. Double-cliquez sur une entité dans l'arborescence ou cliquez sur Ajouter à la liste.

   Les entités de sécurité qui apparaissent dans le champ Noms sont ajoutées à la liste des profils de sécurité.

   Pour ajouter plus de profils, répétez les deux dernières étapes dans la boîte de dialogue Ajouter des profils de sécurité.

5. Cliquez sur OK.

   Le compte ou le groupe d'utilisateurs sélectionné est mappé au profil de sécurité et la boîte de dialogue Autorisations de classes est affichée.

   Remarque : Si vous avez ajouté plusieurs entités de sécurité, la boîte de dialogue Autorisations de classe n'est pas affichée. Vous devez sélectionner le profil dans la boîte de dialogue Profils de sécurité et cliquer sur Autorisations de classes.

6. Dans la boîte de dialogue Autorisations de classes, sélectionnez la classe d'objet à laquelle vous souhaitez attribuer les droits.

   Remarque : Vous pouvez sélectionner plusieurs classes d'objets et spécifier les autorisations de classes pour tous. Pour une sélection continue, appuyez sur la touche Maj et cliquez sur les objets ; pour une sélection aléatoire, appuyez sur la touche Ctrl et cliquez sur les objets.

7. Sélectionnez l'autorisation dans la liste déroulante d'accès aux classes et cliquez sur OK.

   Les autorisations accordées sont affectées au nouveau profil de sécurité.

La boîte de dialogue Ajout de profils de sécurité affiche une liste des autorités de sécurité disponibles : les domaines Windows NT, les cibles d'authentification UNIX, les annuaires externes, tels que NDS, et le sous-système de certificat X.509.

Le gestionnaire stocke la liste des autorités de sécurité disponibles. Lors de l'exécution dans un environnement de domaine Windows NT, le noeud du gestionnaire calcule automatiquement toutes les approbations de domaine explicites disponibles. Vous pouvez afficher la liste des autorités de sécurité disponibles à partir de la boîte de dialogue Ajout de profils de sécurité.

Dans certains cas, vous souhaitez utiliser un domaine approuvé implicitement lors de la création de profils de sécurité, un domaine qui ne se trouve pas directement dans la liste calculée.

La boîte de dialogue Profils de sécurité vous permet d'ajouter et de supprimer des autorités, mais uniquement dans l'espace de nom Windows NT (winnt).

- Pour ajouter un domaine approuvé implicitement, cliquez sur Ajouter et entrez le nom de domaine dans la nouvelle boîte de dialogue.
- Pour supprimer un domaine approuvé implicitement, sélectionnez ce domaine et cliquez sur Supprimer.

Remarque : L'approbation est appliquée par le système d'exploitation. Vous ne pouvez pas ajouter un domaine et que ce domaine soit approuvé par le gestionnaire, sauf si le système d'exploitation approuve déjà le domaine en question.

Types d'accès prédéfinis

L'exemple suivant décrit les résultats de différents droits d'accès sur la classe d'objet Ordinateur :

Accès aux classes	Autorisation résultante
Afficher	Affiche tous les ordinateurs dans le dossier Tous les ordinateurs.
Lecture	Vous permet d'afficher les propriétés des ordinateurs.
Gérer	Vous permet de déployer un package logiciel ou d'exécuter un job sur un ordinateur.
Changement	Vous permet d'ajouter un nouvel ordinateur ou de supprimer un ordinateur.
Contrôle absolu	Vous octroie le contrôle absolu sur les ordinateurs.

Vérification de l'authentification de l'annuaire

Pour vous assurer que l'intégration d'annuaire a été effectuée, vérifiez l'authentification de l'annuaire en vous connectant à Client Automation.

Procédez comme suit: dans l'explorateur DSM :

1. Spécifiez le nom d'utilisateur et le mot de passe

   Définit le nom d'utilisateur pour la connexion.

   Valeur par défaut : Format de nom unique.

   Important : Lorsque vous voulez utiliser des formats UID ou SN pour l'authentification, configurez la valeur de la stratégie de configuration de façon appropriée. Pour plus d'informations, consultez la rubrique Modification de la stratégie pour l'utilisation d'un format de nom d'utilisateur différent (page 399).

2. Sélectionnez l'autorité de sécurité dans la liste suivante :

   Fournisseur de sécurité

   Spécifie le fournisseur de sécurité. Etant donné qu'Client Automation utilise les annuaires externes, le compte utilisateur et les groupes du système d'exploitation pour l'octroi des droits d'accès, le système d'exploitation agit comme fournisseur de sécurité. Sélectionnez le fournisseur de sécurité approprié et le domaine ou l'annuaire Windows correspondant s'affiche.

   Domaine Windows (Windows)/Répertoire (LDAP)

   Sélectionnez le domaine ou l'ordinateur dans lequel se trouve le compte utilisateur. L'annuaire configuré qui peut accéder à Client Automation s'affiche dans la liste déroulante.

3. Cliquez sur Connexion.

   Permet de se connecter au système si les informations d'identification de connexion sont correctes.

Procédez comme suit: avec l'accès à la console Web :

1. Sélectionnez le nom de gestionnaire à partir de la liste déroulante de la console Web.

2. Spécifiez le nom d'utilisateur et le mot de passe

   Définit le nom d'utilisateur pour la connexion. Vous pouvez utiliser le format de nom unique.

   Important : Lorsque vous voulez utiliser les formats UID ou SN pour l'authentification, configurez la valeur de la stratégie de configuration de façon appropriée. Pour plus d'informations, consultez la rubrique Modification de la stratégie pour l'utilisation d'un format de nom d'utilisateur différent (page 399).

3. Sélectionnez l'autorité de sécurité dans la liste suivante :

   Fournisseur de sécurité

   Spécifie le fournisseur de sécurité. Etant donné qu'Client Automation utilise les annuaires externes, le compte utilisateur et les groupes du système d'exploitation pour l'octroi des droits d'accès, le système d'exploitation agit comme fournisseur de sécurité. Sélectionnez le fournisseur de sécurité approprié et le domaine ou l'annuaire Windows correspondant s'affiche.

   Domaine Windows (Windows)/Répertoire (LDAP)

   Sélectionnez le domaine ou l'ordinateur dans lequel se trouve le compte utilisateur. L'annuaire configuré qui peut accéder à Client Automation s'affiche dans la liste déroulante.

4. Cliquez sur Connexion.

   Permet de se connecter au système si les informations d'identification de connexion sont correctes.

Remarque : L'administrateur du gestionnaire de domaines authentifie l'utilisateur avec des droits d'accès à l'annuaire configuré.

Modification de la stratégie pour l'utilisation d'un format de nom d'utilisateur différent

Configurez la valeur de la stratégie de configuration uniquement lorsque vous n'utilisez pas le format de nom unique pour l'authentification. Utilisez la boîte de dialogue Définition des propriétés pour modifier les stratégies de configuration et les adapter à vos besoins et à votre environnement spécifiques.

Remarque : Pour pouvoir modifier une stratégie, vous devez la desceller.

Procédez comme suit:

1. Accédez à Configuration, Stratégie de configuration, Stratégie par défaut de l'ordinateur, DSM, Composants communs, Sécurité, Fournisseurs, Composants, LDAP.
2. Cliquez avec le bouton droit de la souris sur Oracle ldap: Shortname Type (Annuaire LDAP Oracle : type de nom court) dans le volet et sélectionnez Définir les propriétés dans le menu contextuel. Vous pouvez également cliquer sur Définir des propriétés dans le portlet Tâches.

   La boîte de dialogue Définition des propriétés s'ouvre.
3. Dans le champ Valeur, sélectionnez l'*une* des valeurs suivantes selon vos besoins :

   sn

   Spécifie le nom court pour l'annuaire LDAP Oracle.

   uid

   Spécifie l'ID unique de l'annuaire LDAP Oracle.
4. Cliquez sur OK.

   La nouvelle valeur spécifie si le nom d'utilisateur fourni pour l'authentification est sn ou uid.

Remarque : Le nom *sn* doit être unique pour l'annuaire LDAP actif.

Compréhension des attributs de mappage de schémas

Un *mappage de schéma* est un mappage entre des noms d'attributs associés aux objets de données (tels que les utilisateurs, les ordinateurs et les groupes) utilisés dans un répertoire externe et ces noms d'attributs utilisés par les objets DSM correspondants. L'ensemble fixe et standard de noms d'attributs DSM est utilisé afin d'effectuer des requêtes sur les répertoires et de formuler des rapports et des requêtes complexes.

Trois mappages de schéma commun prédéfinis sont également fournis dans Client Automation. Vous avez également la possibilité de créer votre propre schéma personnalisé basé sur le schéma prédéfini.

Noms d'attributs DSM

La table suivante répertorie l'ensemble standard de noms d'attributs, accompagnés de brèves descriptions, utilisés par des applications basées sur DSM pour effectuer des requêtes sur les répertoires :

Nom de l'attribut	Description
Classe-objet	Classe des objets
dc	Contrôleur de domaine
o	Organisation
ou	Unité organisationnelle
c	Country
m	Emplacement
userDn	Nom unique de l'utilisateur
userCn	Nom usuel de l'utilisateur
userSn	Nom de famille de l'utilisateur
givenName	Nom donné de l'utilisateur
displayName	Nom d'affichage
userName	Nom d'utilisateur
userID	Identificateur d'utilisateur
userPassword	Mot de passe de l'utilisateur
memberOf	Noms/ noms uniques des groupes dont un utilisateur est membre
directReports	Noms/ noms uniques des personnes qui envoient des rapports à cet utilisateur
streetAddress	Rue
postalCode	Code postal
Company (société)	Société
Service	Service
email	Adresse électronique
telephoneNumber	Numéro de téléphone
jobTitle	Titre du poste
userDescription	Description de l'utilisateur
assetDn	Nom unique de l'ordinateur

Nom de l'attribut	Description
assetCn	Nom usuel de l'ordinateur
assetName	Nom de l'ordinateur
dnsHostName	Nom d'hôte DNS
operatingSystem	Système d'exploitation
operatingSystemServicePack	Service Pack OS
operatingSystemVersion	Version OS
assetDescription	Description de l'ordinateur
groupDn	Nom unique du groupe
groupCn	Nom usuel du groupe
groupName	Nom du groupe
groupMembers	Noms/ noms uniques des utilisateurs membres de ce groupe
groupDescription	Description du groupe.

En outre, le mappage de schéma DSM contient des champs qui ne sont pas des noms d'attributs. Ce sont les noms des classes d'objets que les applications basées sur DSM utilisent :

- L'interface utilisateur graphique utilise computerMap, groupMap et userMap pour déterminer le type de nœuds à afficher.
- Le job de synchronisation de répertoires utilise userMap et computerMap.

Le mappage de schéma DSM contient les champs suivants :

computerMap

Correspond au nom objectClass représentant un ordinateur dans le répertoire configuré.

groupMap

Correspond au nom objectClass représentant un groupe dans le répertoire configuré.

userMap

Correspond au nom objectClass représentant un utilisateur dans le répertoire configuré.

containerMap

Correspond au nom de classe pour *conteneur*.

Schéma Active Directory

Le tableau suivant indique le mappage de noms d'attribut Active Directory au schéma DSM :

Nom de l'attribut DSM	Nom d'attribut Active Directory
Classe-objet	Classe-objet
dc	dc
c	c
m	m
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	memberOf
directReports	directReports
streetAddress	streetAddress
postalCode	postalCode
Company (société)	Company (société)
Service	Service
email	mail
telephoneNumber	telephoneNumber
jobTitle	titre
userDescription	description
assetCn	cn
assetName	name
dnsHostName	dnsHostName
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion

Nom de l'attribut DSM	Nom d'attribut Active Directory
assetDescription	description
groupCn	cn
groupName	name
groupMembers	Membre
groupDescription	description
containerMap	conteneur
groupMap	groupe
userMap	Utilisateur
computerMap	ordinateur
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–
userDn*	distinguishedName
groupDn*	distinguishedName
assetDn*	distinguishedName
o*	o
ou*	ou

*** Remarque :** Le mappage de ces attributs est fixe et ne peut être modifié. Cependant, vous pouvez utiliser ces noms d'attributs DSM dans des requêtes.

Schéma d'annuaire Oracle

Le tableau suivant indique le mappage de noms d'attribut d'annuaire Oracle au schéma DSM :

Nom de l'attribut DSM	Nom d'attribut Oracle
Classe-objet	Classe-objet
dc	dc
c	c
m	m
userCn	cn
userSn	Sn
givenName	givenName

Nom de l'attribut DSM	Nom d'attribut Oracle
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress
postalCode	postalCode
Company (société)	Company (société)
Service	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	titre
userDescription	description
assetCn	cn
assetName	name
dnsHostName	hôte
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	Membre
groupDescription	description
containerMap	conteneur
groupMap	groupOfUniqueNames
userMap	inetOrgPerson
computerMap	ordinateur
uniqueUserFields 1 – uniqueUserFields 5	–

Nom de l'attribut DSM	Nom d'attribut Oracle
uniqueComputerFields 1 – uniqueComputerFields 5	–

*** Remarque :** Le mappage de ces attributs est fixe et ne peut être modifié. Cependant, vous pouvez utiliser ces noms d'attributs DSM dans des requêtes.

Schéma eTrust Directory

Le tableau suivant indique le mappage de noms d'attribut eTrust Directory au schéma DSM :

Nom de l'attribut DSM	Nom d'attribut eTrust Directory
Classe-objet	Classe-objet
dc	dc
c	c
m	m
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress
postalCode	postalCode
Company (société)	Company (société)
Service	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	titre
userDescription	description

Nom de l'attribut DSM	Nom d'attribut eTrust Directory
assetCn	cn
assetName	name
dnsHostName	hôte
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	Membre
groupDescription	description
containerMap	conteneur
groupMap	groupOfNames
userMap	inetOrgPerson
computerMap	device
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–
userDn*	dn
groupDn*	dn
assetDn*	dn
o*	o

*** Remarque :** Le mappage de ces attributs est fixe et ne peut être modifié. Cependant, vous pouvez utiliser ces noms d'attributs DSM dans des requêtes.

Intégration du répertoire dans CA Client Automation

Pour obtenir une liste détaillée des services d'annuaire pris en charge, consultez la matrice de compatibilité.

Chapitre 11: Fonctionnalités de sécurité Client Automation

Les fonctionnalités de sécurité dans Client Automation couvrent deux zones.

Authentification

Garantit que l'objet demandeur est bien ce qu'il déclare être.

Autorisation

Permet de configurer et valider les droits et permissions d'accès pour les opérations concernant des objets sécurisés.

Ce chapitre traite des sujets suivants :

Authentification

L'authentification identifie les membres d'une base informatique sécurisée, basée sur les informations d'identification fournies.

Les membres d'une base informatique sécurisée sont :

Utilisateurs et appartenance indirecte à un groupe

Il s'agit avant tout d'entités homogènes de sécurité du système d'exploitation en cours. Il peut s'agir, par exemple, d'utilisateurs Windows (Active Directory, domaine ou locaux), UNIX (LDAP) ou d'utilisateurs locaux UNIX.

Ordinateurs

Les ordinateurs qui font partie d'une base informatique sécurisée, notamment Windows NT, peuvent être identifiés et authentifiés. En théorie, les ordinateurs UNIX peuvent être identifiés, car ils font également partie d'une base informatique sécurisée avec laquelle il est possible d'établir une relation sécurisée.

Différentes informations répertoriées ci-dessous sont utilisées pour authentifier un utilisateur ou un ordinateur.

- Dans les environnements d'exploitation Windows :
  - Nom d'utilisateur
  - Mot de passe
  - Domaine Windows
  - Fournisseur de sécurité
- Dans des environnements d'exploitation Linux et UNIX :
  - Nom de l'ordinateur
  - Nom d'utilisateur
  - Mot de passe
  - Fournisseur de sécurité

Différentes applications disposent d'exigences différentes en matière d'authentification. Si possible, une connexion unifiée est utilisée : les informations d'identification actuelles de l'utilisateur sont utilisées de manière implicite plutôt que d'inviter l'utilisateur à fournir des informations d'identification explicites.

Cependant, dans certains cas, ces informations d'identification ne sont pas valides pour la ressource à laquelle elles accèdent ou les opérations spéciales peuvent requérir une nouvelle authentification. Lorsqu'une connexion unifiée ne doit pas être utilisée ou que les informations d'identification ne sont pas valides, une application de l'interface utilisateur graphique peut demander des informations d'identification chaque fois qu'elles sont requises, tandis qu'une application de ligne de commande en cours d'exécution en mode de traitement par lot échoue et enregistre une erreur d'authentification.

Si vous utilisez un fournisseur de sécurité LDAP pour authentifier les utilisateurs dans un répertoire lorsque vous spécifiez des informations d'identification, assurez-vous de la validité de ces informations d'identification pour le répertoire cible et de leur spécification complète. Pour Active Directory, vous devez utiliser le DN LDAP complet, par exemple :

```
CN=user,OU=Users,OU=myOU,DC=mydomain,DC=com
```

Lors de l'utilisation de répertoires LDAP externes génériques pour l'authentification, les objets d'authentification doivent bénéficier directement de droits d'accès, car les membres des groupes ne peuvent pas être évalués directement. Cela ne s'applique pas à Active Directory.

Formats de nom d'utilisateur pris en charge

Les formats de nom d'utilisateur suivants sont pris en charge par Client Automation. Ces formats de nom s'appliquent à toutes les applications CA Technologies qui requièrent un nom d'utilisateur, telles que l'interface utilisateur graphique de l'explorateur et les services Web.

Sécurité native Windows ou sécurité locale Linux/UNIX (ce qui signifie utilisateurs locaux et domaines sécurisés)

Format de nom d'utilisateur : *username* (format de niveau inférieur Windows NT ou utilisateur Linux)

LDAP communique avec Active Directory (Windows et Linux/UNIX)

Format de nom d'utilisateur : UPN ou DN

LDAP communique avec un répertoire (sauf Active Directory) (Windows et Linux/UNIX)

Format de nom d'utilisateur : DN

Format de nom d'utilisateur : UID ou SN (pour annuaire LDAP Oracle)

Authentification basée sur un certificat X.509

Chaque fois qu'un processus client Client Automation se connecte à un module d'extension CAF nécessitant une authentification, le processus client doit transférer les informations d'identification de sécurité répondant aux exigences de sécurité des services cible. Lorsque le processus client est en cours d'exécution en tant que processus autonome, comme un service Windows NT ou un démon UNIX, le processus client peut procéder à l'authentification à l'aide de certificats V3 X.509 en l'absence d'informations d'identification utilisateur.

Un certificat X.509 pour une authentification Client Automation comprend un ensemble de paires attribut-valeur compilées avec la clé de chiffrement publique d'une paire de clés asymétriques. Le certificat dispose d'une signature numérique et il est scellé par un certificat de l'utilisateur racine. Le certificat enregistre le nom de l'objet pour lequel le certificat a été émis, le nom de l'autorité émettrice du certificat et les informations portant sur l'expiration. Le nom unique (DN) se réfère souvent au nom d'objet. Le nom d'objet est mappé sur un Uniform Resource Identifier (URI) dans l'espace de nom x509cert, comme suit :

```
x509cert://dsm r11/CN=Basic Host Identity,O=Computer Associates,C=US
```

Pour obtenir une présentation des certificats actuels, reportez-vous à Certificats communs (page 583) et Certificats spécifiques à l'application (page 584).

Grâce à la cryptographie de la clé publique, les clients s'authentifient eux-mêmes sur demande auprès de serveurs de modularité. Un serveur de modularité peut donc utiliser l'identité certifiée pour effectuer des vérifications d'autorisations ultérieures et valider des enregistrements d'audit. La console de gestion permet l'affectation de privilèges de tâches ou d'objets aux URI de certificat dans la base de données de gestion Client Automation.

Sécurité du niveau de l'objet et certificats

La base de données de gestion Client Automation fournit la classe et la sécurité du niveau de l'objet (OLS). Les autorisations attribuées dans la base de données sont associées à un profil de sécurité ; elles sont représentées par un URI d'objet. Les URI de certificat peuvent être associés aux profils de sécurité et, par conséquent, être utilisés pour contrôler l'accès à la base de données de gestion Client Automation.

Par exemple, lorsque des serveurs de modularité se connectent à un gestionnaire de domaines, ils s'authentifient eux-mêmes grâce au certificat d'enregistrement. L'URI associé au certificat d'enregistrement a reçu uniquement les autorisations suffisantes dans la base de données pour permettre l'enregistrement du nœud du serveur de modularité.

Certificats root

Client Automation utilise des certificats de l'utilisateur racine sécurisés pour valider les certificats utilisés pour l'authentification. Plusieurs certificats racines peuvent être utilisés en parallèle pour autoriser la gestion de différentes chaînes d'autorité ou pour aider à la migration d'une chaîne de certificat vers une nouvelle chaîne.

Pour que deux nœuds communiquent avec succès et s'authentifient ensuite, le nœud authentificateur (répondeur) requiert l'accès au certificat de l'utilisateur racine qui a signé le certificat de la partie en cours d'authentification (initiateur). Si le certificat n'est pas disponible, non reconnu ou non valide, l'authentification échoue. Au cours de la migration planifiée du certificat, l'authentificateur peut être mis à jour grâce à un ou plusieurs certificats de l'utilisateur racine sécurisés, pour autoriser la migration par étapes des clients. Les initiateurs disposant de différentes versions de certificats s'authentifient toujours avec succès s'ils sont signés par des certificats de l'utilisateur racine sécurisés par le répondeur.

Stockage de certificats

Les certificats d'authentification sont stockés de manière sécurisée sur chaque nœud Client Automation. Les fichiers de certificat sont protégés par un mot de passe ; le mot de passe d'utilisation est chiffré à l'aide de la configuration Client Automation.

Certificats d'identité de l'hôte standard

Chaque nœud Client Automation dispose d'un certificat qui fournit une identité d'hôte standard (BHI) installée par défaut. D'autres certificats sont installés avec les services qui les requièrent pour des objectifs précis (reportez-vous à la section Certificats actuels (page 583)). L'installation de CA Client Automation est accompagnée d'un certificat standard par défaut signé par un certificat de l'utilisateur racine Client Automation. Ce certificat est installé sur chaque nœud Client Automation dans l'entreprise.

Vous recommandons aux utilisateurs finaux d'envisager la création de leur propre certificat de l'utilisateur racine, des certificats d'identité d'hôte standard (BHI) et des certificats spécifiques à l'application. Pour plus d'informations sur le remplacement des certificats par défaut par des certificats spécifiques aux utilisateurs finaux, consultez "Comment introduire vos propres certificats X.509 dans l'image d'installation" (page 235).

Lors de la création de nouveaux certificats BHI, il existe trois paradigmes principaux :

- Création d'un certificat d'identité d'hôte unique utilisé sur tous les nœuds Client Automation dans l'entreprise. Il s'agit de la solution la plus simple car l'image d'installation personnalisée doit être générée seulement une fois pour créer un package personnalisé.

- Créez un certificat d'identité d'hôte unique pour chaque noeud individuel dans l'entreprise DSM. Il s'agit de la solution la plus complexe. Le DN attribué à chaque nœud doit être unique et refléter l'identité de l'ordinateur hôte. Un nom d'hôte complet convient généralement à cet objectif. Une image d'installation personnalisée est requise pour installer le fichier de certificat approprié sur l'ordinateur cible.
- Un hybride des deux paradigmes se trouve ci-dessus. Création d'un certificat d'identité d'hôte unique à utiliser sur la majorité des nœuds Client Automation. Créez des certificats d'identité personnalisés à utiliser sur un serveur de modularité et des noeuds du gestionnaire DSM. Lorsqu'une exigence pour un certificat personnalisé est identifiée, émettez un nouveau certificat et installez-le sur le nœud spécifié. Il s'agit de la solution la plus flexible. Les nœuds importants de l'entreprise sont identifiés et protégés de manière plus efficace.

Distribution de certificat

La distribution de certificat doit être couverte avant la création de certificat. En fonction de la méthode de création de certificat choisie (voir la description dans Certificats d'identité de l'hôte standard (page 411)), la distribution de certificat peut se révéler assez complexe.

Client Automation ne fournit aucune technologie de distribution de certificat automatisée. Il est livré avec des certificats par défaut pour chaque nœud et des certificats spécifiques à l'application Client Automation.

Pour migrer à partir des certificats par défaut après une installation par défaut, les certificats doivent être distribués de la manière suivante (simplifiée). Cela permet une migration sécurisée réussie ne causant aucun temps d'arrêt dans les communications et l'authentification, du fait de l'utilisation parallèle de l'utilisateur racine sécurisés.

1. Créez un nouveau certificat de l'utilisateur racine. Assurez-vous que le nom root (DN) est différent de celui du certificat de l'utilisateur racine Client Automation existant.
2. Planifiez la distribution du nouveau certificat codé DER de l'utilisateur racine vers tous les nœuds dans l'infrastructure Client Automation. Cela active l'utilisateur racine en tant qu'autorité de l'utilisateur racine sécurisée vers tous les nœuds Client Automation.
3. Créez de nouveaux profils de sécurité dans la base de données de gestion Client Automation pour remplacer les profils de certificats spécifiques à l'application existants. Ne supprimez pas encore les anciens profils.
4. Planifiez la distribution de nouveaux certificats vers tous les nœuds Client Automation.

5. Lorsque la distribution de certificat est réussie, planifiez la suppression des certificats Client Automation précédents.
6. Supprimez les anciens profils de sécurité pour les certificats spécifiques à l'application.

Cette liste n'est pas exhaustive. Contactez le support technique de CA Technologies pour obtenir des informations sur la distribution de certificat à grande échelle et sur le remplacement par une implémentation PKI à l'échelle maximale.

Création de nouveaux certificats

Pour créer de nouveaux certificats, vous pouvez utiliser l'outil cacertutil fourni ou une PKI existante pour générer des certificats à votre intention. L'utilisation de systèmes PKI externes sort du cadre de cette documentation, mais les exigences relatives aux certificats sont les mêmes que pour la création d'un certificat avec cacertutil.

Remarque : Une PKI externe ne nécessite pas la création d'un nouveau certificat de l'utilisateur racine pour l'infrastructure Client Automation.

Génération d'un nouveau certificat root

Lors de la génération d'un nouveau certificat de l'utilisateur racine, les deux formes suivantes du certificat doivent être créées :

- Un fichier codé PKCS#12. Il contient à la fois la section publique du certificat et la clé privée.
- Un fichier codé DER. Il contient uniquement la partie du certificat accessible publiquement.

Les deux formes du certificat sont générées au même moment grâce à l'outil Client Automation. Lors de l'utilisation d'une PKI externe, le certificat de l'utilisateur racine peut être exporté au format DER.

Le nouveau certificat de l'utilisateur racine est crucial pour la sécurité dans Client Automation et, en tant que tel, doit être protégé de toute divulgation accidentelle ou délibérée. Le fichier de certificat PKCS#12 doit être protégé par une phrase de passe complexe et doit être stocké dans un emplacement de stockage de données administratives sécurisé.

Le certificat au format PKCS#12 est utilisé pour signer d'autres certificats. Le certificat au format DER est utilisé pour vérifier ces certificats signés.

La commande de création d'un nouveau certificat de l'utilisateur racine a le format suivant :

```
cacertutil create -o:rootname.p12 -od:rootname.der -op:passphrase "-
s:CN=YourRoot,O=YourOrg,C=Country" -d:NumberOfDays -oe
```

-o

Spécifie le *filename* de sortie pour le certificat compilé PKCS#12.

-od

Spécifie le *filename* de sortie pour le certificat codé DER.

-op

Spécifie une phrase de passe utilisée pour chiffrer le fichier de certificat PKCS#12.

-s

Spécifie l'objet du certificat.

-d

Spécifie la durée de vie du certificat en jours (par exemple, 730 (= 2 années)).

-oe

Génère une version chiffrée aléatoire de la phrase de passe utilisée pour décoder le certificat et l'envoie vers la console. Cette phrase de passe chiffrée peut être fournie à l'outil du certificat à la place d'un mot de passe en texte clair.

Génération de certificats spécifiques à l'application

Pour chaque application répertoriée dans Certificats actuels (page 583), créez un nouveau certificat. Si vous n'utilisez pas le DN comme répertorié dans la table d'annexe, vous devrez également attribuer les autorisations requises pour le profil de sécurité du certificat dans le navigateur de sécurité Client Automation.

Pour garantir que le navigateur de sécurité Client Automation peut visualiser le certificat nouvellement créé, le certificat codé DER doit être importé dans la base de données de certificat Client Automation sur les nœuds du gestionnaire.

La commande permettant de créer les nouveaux certificats est la suivante :

```
cacertutil create -o:certname.p12 -od:certname.der -op:passphrase "-s:CertDN" -
i:rootname.p12 -ip:rootpassphrase -d:730
```

-o

Spécifie le nom du fichier de sortie pour le certificat compilé PKCS#12.

-od

Spécifie le nom du fichier de sortie pour le certificat codé DER.

-op

Spécifie la phrase de passe pour protéger le certificat de sortie PKCS#12.

-s

Spécifie le DN vers lequel le certificat doit être émis.

-i

Spécifie le nom du fichier du certificat de l'utilisateur racine PKCS#12.

-ip

Spécifie la phrase de passe qui protège le certificat de l'utilisateur racine PKCS#12.

-d

Spécifie la durée de vie du certificat en jours (l'exemple montre 2 années (= 730 jours)).

Génération du certificat d'identité de l'hôte standard

Le certificat d'identité de l'hôte standard (BHI) ne dispose d'aucun droit pour la base de données de gestion Client Automation et d'aucun profil de sécurité associé dans l'installation par défaut. Par conséquent, le choix d'un nouveau DN pour le certificat n'implique aucune opération supplémentaire pour modifier les profils et les autorisations de sécurité Client Automation.

Le DN par défaut attribué au certificat BHI se présente comme suit :

CN=Basic Host Identity,O=Computer Associates,C=US

La commande de création d'un nouveau certificat d'identité de l'hôte standard a le format suivant :

```
cacertutil create -o:certname.p12 -od:certname.der -op:passphrase “-s:CertDN” -
i:rootname.p12 -ip:rootpassphrase -d:730
```

-o

Spécifie le nom du fichier de sortie pour le certificat compilé PKCS#12.

-od

Spécifie le nom du fichier de sortie pour le certificat codé DER.

-op

Spécifie la phrase de passe pour protéger le certificat de sortie PKCS#12.

-s

Spécifie le DN vers lequel le certificat doit être émis.

-i

Spécifie le nom du fichier du certificat de l'utilisateur racine PKCS#12.

-ip

Spécifie la phrase de passe qui protège le certificat de l'utilisateur racine PKCS#12.

-d

Spécifie la durée de vie du certificat en jours (l'exemple montre 2 années (= 730 jours)).

Installation de nouveaux certificats

Lors de l'installation de nouveaux certificats sur un noeud Client Automation, le processus qui installe le certificat doit être en cours d'exécution en tant qu'administrateur local, à savoir un membre du groupe d'administrateurs sous Windows.

Installation d'un nouveau certificat root

Pour installer un nouveau certificat de validation de l'utilisateur racine sur un nœud Client Automation, utilisez le fichier codé DER. La commande d'installation de ce certificat a le format suivant :

```
cacertutil import -i:rootcert.der -ip:passphrase -it:X509V3
```

Cela importe les informations accessibles publiquement du certificat en tant que certificat de l'utilisateur racine sécurisé dans la base de données du certificat.

Installation de certificats spécifiques à l'application

Dans la base de code CA Client Automation, les certificats spécifiques à l'application sont référencés par un nom de balise plutôt que par les DN attribués aux certificats. Les noms de balise pertinents sont détaillés dans Certificats actuels (page 583). Le certificat doit être installé uniquement sur les noeuds qui les requièrent pour s'authentifier sur un serveur de modularité ou un gestionnaire DSM.

La commande d'installation d'un certificat spécifique à une application a le format suivant :

```
cacertutil import -i:certname.p12 -ip:passphrase -t:tagname
```

-i

Spécifie le nom du fichier de certificat PKCS#12 à importer.

-ip

Spécifie la phrase de passe utilisée pour protéger le certificat.

-t

Spécifie le nom de balise du certificat.

Pour que le navigateur de sécurité DSM visualise le certificat, le certificat codé DER doit être importé dans la base de données du certificat sur les noeuds du gestionnaire. La commande d'importation d'un certificat codé DER a le format suivant :

```
cacertutil import -i:certname.der -it:X509V3
```

-i

Spécifie le nom du certificat codé DER à importer.

-it

Spécifie le type de certificat à importer. X509V3 spécifie le codage DER.

Installation du certificat d'identité de l'hôte standard

Le certificat d'identité de l'hôte standard est toujours installé avec le dsmcommon du nom de balise. La commande d'installation du certificat BHI a le format suivant :

```
cacertutil import -i:certname.p12 -ip:passphrase -t:dsmcommon -h
```

-i

Spécifie le nom du fichier du certificat d'entrée PKCS#12.

-ip

Spécifie la phrase de passe utilisée pour protéger le certificat d'entrée.

-t

Spécifie le nom de balise du certificat.

-h

Spécifie que le certificat doit être utilisé pour fournir l'identité de l'hôte par défaut.

Remplacement de certificat

Le remplacement des certificats Client Automation par défaut nécessite que tout nouveau certificat utilise les mêmes noms de fichier physiques que ceux d'origine. Les noms d'objet affectés aux certificats n'ont pas besoin d'être identiques à l'original. Ceux-ci sont enregistrés et contrôlés par le fichier d'installation cfcert.ini. Ils sont ensuite insérés dans la base de données au cours de l'installation, en fonction des instructions du fichier.

Le tableau suivant répertorie les noms de fichier et leur association :

Nom du fichier	Associé au sujet Client Automation
itrm_dsm_r11_root.der	Certificat racine
basic_id.p12	Certificat d'identité d'hôte standard
dsmpwchgent.p12	Accès à l'entreprise
dsmpwchgdom.p12	Accès au domaine
dsmpwchgrep.p12	Accès au générateur de rapports
ccsm.p12	Accès à CSM
itrm_dsm_r11_cmdir_eng.p12	Accès à la synchronisation des répertoires
registration.p12	Accès à l'enregistrement
itrm_dsm_r11_sd_catalog.p12	Accès au catalogue SD
itrm_dsm_r11_agent_mover.p12	Accès au déplacement de l'agent SD

Suppression de certificat

Les certificats peuvent être supprimés un à la fois ou en bloc.

Pour supprimer un certificat de manière individuelle, émettez la commande suivante :

```
cacertutil remove -s:nom_objet [-t:nom_balise] [-l:{local|global}]
```

-s

Spécifie le nom de l'objet vers lequel le certificat est émis.

-t

Spécifie le nom de balise du certificat, en cas d'installation avec un nom de balise.

-l

Spécifie si le certificat a été installé dans l'emplacement de stockage commun global ou local.

La commande de suppression en bloc des certificats se présente comme suit :

```
purge cacertutil
```

Important : Cette commande supprime toutes les entrées de certificat du magasin commun aussi bien pour l'utilisateur actuel que pour l'ordinateur local (si l'utilisateur du processus actuel dispose des droits suffisants pour cela).

Sécurité et authentification VMware ESX

L'agent distant AM de Client Automation prend uniquement en charge les serveurs Vmware ESX en cours d'exécution dans le mode HTTP sécurisé. VMware recommande l'utilisation de HTTPS (HTTP sécurisé, activé par défaut) pour le déploiement de production. C'est pour cette raison que l'agent distant AM se connecte uniquement aux hôtes ESX sur lesquels la configuration par défaut recommandée pour HTTPS est utilisée.

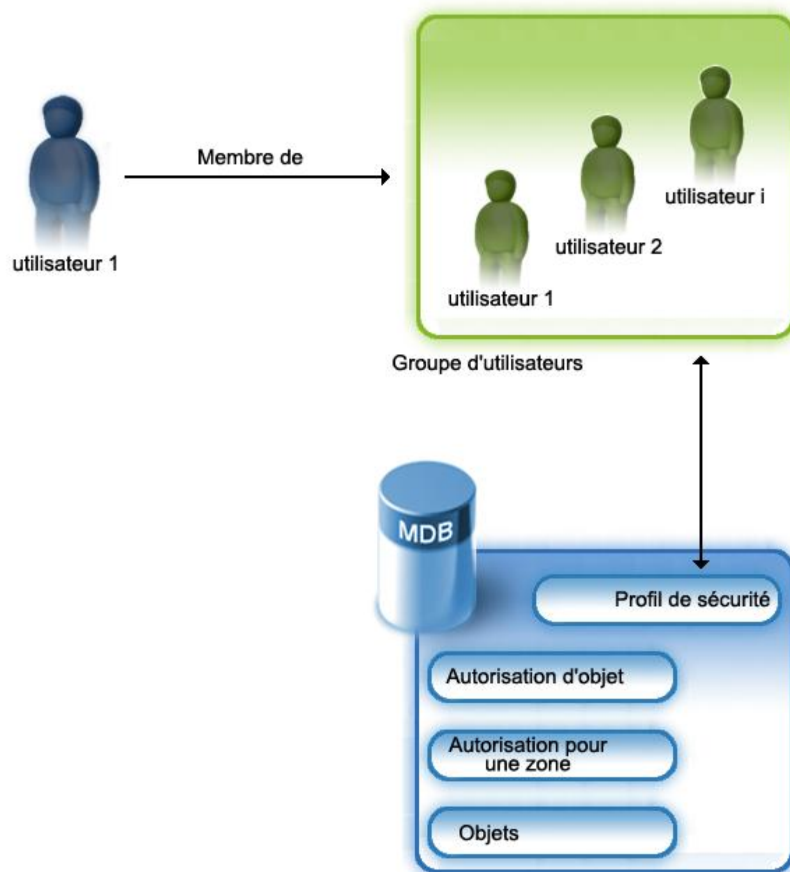
Le protocole SSL (Secure Sockets Layer) est utilisé comme pour la connexion entre l'agent DSM et l'ordinateur hôte ESX. Toutefois, l'identité d'un ordinateur hôte ESX n'étant pas connue à l'avance, aucune authentification n'a lieu entre l'agent DSM et l'hôte ESX. Les certificats ne seront pas utilisés pour l'authentification d'un hôte d'ESX.

Autorisation

L'autorisation contrôle les droits et les privilèges pour un objet associé à une entité authentifiée, généralement un utilisateur connecté. une entité authentifiée est gérée par des profils de sécurité. Cela signifie qu'un utilisateur ou un groupe d'utilisateurs est représenté par un profil de sécurité et que l'ensemble des autorisations sont gérées avec ce profil de sécurité.

Le sous-système de sécurité Client Automation gère l'autorisation en fournissant une option de sécurité fiable et générique pour l'CA Client Automation entier. Il est responsable du contrôle des droits et des privilèges pour un objet associé à une entité authentifiée, appelée profil de sécurité.

L'illustration suivante fournit un aperçu du sous-système de sécurité qui gère l'autorisation :



En général, un utilisateur connecté à un système est membre d'un ou de plusieurs groupes d'utilisateurs, où le groupe d'utilisateurs est représenté par un profil de sécurité.

Cela signifie que l'administrateur Client Automation est responsable de la création du profil de sécurité pour un groupe d'utilisateurs ou le profil de sécurité distinct d'un utilisateur spécifique.

Les autorisations pour les profils de sécurité sur les objets sont également stockées dans la MDB, en plus des objets Client Automation.

Vous pouvez, par exemple, créer des profils de sécurité pour déterminer quels utilisateurs et quels groupes dépendants du système d'exploitation peuvent accéder au système Client Automation. Vous pouvez également établir des autorisations de classes, ainsi que des autorisations de groupe et des autorisations sur l'objet. Vous pouvez limiter l'accès des utilisateurs ou des groupes d'utilisateurs aux dossiers ou objets sélectionnés.

Profils de sécurité

Un profil de sécurité est un compte ou un groupe d'utilisateurs du système d'exploitation dans le gestionnaire de domaines (profils locaux) ou dans son domaine réseau (profil de domaine).

Le sous-système de sécurité dans Client Automation prend en charge plusieurs profils de sécurité. Un profil de sécurité est soit intégré (créé lors de l'installation), soit défini par l'utilisateur.

Un profil de sécurité défini par l'utilisateur représente un utilisateur unique ou un groupe d'utilisateurs.

Les profils de sécurité les plus importants créés lors de l'installation incluent :

- Propriétaire (compte virtuel)
- Tout le monde (compte virtuel par défaut pour tout le monde)

En plus du profil de sécurité, il existe un ensemble de classes de sécurité, associées à un profil. Chaque profil possède son propre ensemble de classes de sécurité. Une classe de sécurité permet de paramétrer des autorisations qui sont ensuite affectées à une instance d'une telle classe, dès sa création.

Vous pouvez également créer des profils de sécurité pour les utilisateurs dans les domaines sécurisés. Chaque utilisateur doit disposer d'un profil de sécurité valide pour se connecter au système. Si de nouveaux utilisateurs sont ajoutés à un groupe géré, ils héritent automatiquement des droits d'accès accordés au groupe et peuvent se connecter au système instantanément.

Un utilisateur peut disposer de plusieurs profils. Cependant, chaque profil peut être mappé sur un utilisateur ou un groupe uniquement. Si, par exemple, un utilisateur est membre d'un groupe, alors cet utilisateur peut posséder deux profils : un profil mappé au compte utilisateur et l'autre mappé au groupe. Dans ce cas, l'utilisateur dispose des autorisations pour les deux profils.

Si un utilisateur est membre de plusieurs profils de sécurité, l'autorisation effective pour cet utilisateur est une union (mathématique) de chacune des autorisations individuelles définies pour chaque profil de sécurité (comme l'application de l'opérateur OU (mathématique) à toutes les autorisations).

Si vous souhaitez refuser l'accès à un utilisateur d'un profil de sécurité individuel, vous devez supprimer cet utilisateur du profil de sécurité.

Le système propose des profils de sécurité prédéfinis et vous permet de créer autant de profils que vous le souhaitez, à l'aide de la boîte de dialogue Profils de sécurité.

Nous vous recommandons qu'au moins l'un de ces profils ait un contrôle total du droit d'accès au système.

Présentation des autorisations

L'autorisation couvre les types d'autorisation suivants :

- Autorisations de classes
- Autorisations sur l'objet
- Autorisations pour une zone

Le sous-système de sécurité gère tous les types d'autorisations et utilise une approche cumulative afin d'obtenir des autorisations effectives.

Si vous avez activé les autorisations pour une zone, deux types d'autorisations (d'objet et de zone) sont vérifiés pour accéder aux objets. Cela signifie qu'un utilisateur nécessite des autorisations pour un objet *et* pour une zone afin d'obtenir un objet géré. Les autorisations pour un objet sont vérifiées uniquement si la prise en charge de zone est désactivée.

Autorisations de classes

Les autorisations de classes correspondent aux droits d'accès que vous spécifiez au niveau des classes. Cela signifie que les autorisations au niveau de la classe correspondent aux droits par défaut pour chaque objet constituant une instance de cette classe.

Lorsque vous créez un profil de sécurité, vous devez spécifier les autorisations de classes pour chaque profil de sécurité. Pour toutes les classes de sécurité, Aucun accès est défini par défaut. Les profils de sécurité disposant des autorisations de classes appropriées vous confèrent des droits d'accès au système. Vous pouvez spécifier ces informations dans la boîte de dialogue Autorisations de classes.

Les autorisations de classes s'appliquent globalement à tous les objets d'une classe d'objet. Si vous souhaitez limiter les utilisateurs à un objet ou à un dossier spécifique de l'Explorateur, ou leur accorder des droits d'accès étendus, utilisez respectivement les boîtes de dialogue Autorisations sur l'objet ou Autorisations du groupe de sécurité.

Les classes de sécurité servent à regrouper des objets de type identique. Le sous-système de sécurité dans CA Client Automation prend en charge les classes de sécurité suivantes :

- Matériel détecté (Ordinateur)
- Utilisateurs
- Utilisateurs
- Gestionnaire
- Serveurs
- Groupes d'actifs
- Groupes de serveurs
- Groupes de domaines
- Requêtes
- Classes de sécurité
- Profils de sécurité
- Packages logiciels
- Procédures logicielles
- Groupes de procédures
- Conteneurs de job
- Jobs logiciels
- Jobs d'actifs
- Modules
- Règles basées sur une requête
- Stratégies basées sur les événements
- Images de démarrage OSIM
- Images de système d'exploitation OSIM
- Moteur
- Ordinateur de stratégies de configuration
- Utilisateur de stratégies de configuration
- Accès aux répertoires externes
- Modèles de rapports
- Modules d'inventaire

Les classes de sécurité suivantes sont uniquement utilisées au niveau de la classe.

- MDB Access
- Activez le Panneau de configuration
- Activez Remote Control

La sécurité au niveau de la classe signifie que chaque objet ou instance d'une classe obtient l'autorisation, comme défini pour la classe par défaut.

Autorisations de classes combinées requises pour des actions spécifiques

Quelques droits de classe d'objet dépendent les unes des autres ; cela signifie que pour réaliser les actions suivantes, vous devez accorder des droits à plus d'une classe d'objet.

Modèles de rapports

Pour planifier un modèle Rapport, vous devez accorder la modification à la classe d'objet "Planification de rapport" *et* la modification pour la classe d'objet "Moteur".

Profils de sécurité

La classe d'objet "Profils de sécurité" contrôle la gestion avec des profils de sécurité uniquement (supprimer, etc.). Si vous voulez modifier des autorisations de classes d'objets dans un profil de sécurité, vous devez disposer d'un accès spécial (VRWXP, avec l'autorisation P) pour la classe d'objet "Autorisations de classe".

Moteur

Pour relier une tâche de moteur à un moteur, vous devez accorder Modifier à la classe d'objet "Moteur" *et* Gérer à la classe d'objet "Tâche de moteur".

Concernant la sécurité de moteur, si vous voulez démarrer, arrêter ou modifier des objets de moteur, vous devez accorder un Contrôle total à la classe "Moteur" dans le profil de sécurité *et* au-delà des droits Administrateur NT ou racines à l'ordinateur sur lequel est exécuté le moteur.

Sécurité de job logiciel

Pour modifier ou supprimer un job logiciel sous le dossier /computer, le logiciel est livré dans /Jobs/Software Jobs ; les classes d'objets Ordinateur et Job logiciel doivent disposer de droits Modifier.

Sécurité de procédure

Si vous voulez démarrer, arrêter ou modifier des objets Procédure, vous devez accorder Modifier (VRWXD) à la classe "Procédure" *et* au-delà des autorisations de fichier administrateur/utilisateur racine.

Prise en charge des zones de sécurité

Si vous souhaitez activer ou désactiver la prise en charge des zones de sécurité et définir les zones de sécurité par défaut, les autorisations de classe pour la classe de l'objet "Zone de sécurité" doivent être configurées au moins sur Accès spécial (VP).

Si vous souhaitez lier les profils de sécurité à une zone de sécurité, les autorisations Affichage (V) sont suffisantes pour la classe d'objet "Zone de sécurité". Les autorisations de classe pour les classes d'objets "Profils de sécurité" doivent être configurées au moins sur Accès spécial (VW).

Autorisations d'objet

La définition des autorisations sur l'objet est utile lorsque vous souhaitez limiter les droits d'accès d'un objet particulier. Par défaut, tous les objets héritent des autorisations définies pour la classe d'objets.

Les autorisations d'objets sont prioritaires sur les autorisations de classes et de groupes.

Les autorisations d'objet sont toujours présentes et gérées par le sous-système de sécurité. Elles ne peuvent être désactivées. Si vous ne voulez pas vous charger des autorisations d'objet, vous pouvez définir des autorisations au niveau de la classe pour toutes les classes d'objets par Contrôle complet.

L'autorisation est basée sur le concept d'une entrée de contrôle d'accès (ACE). ACE représente n'importe quelle combinaison de lettres indiquée dans le tableau suivant, notamment VR. Cette ACE vous permet d'afficher et de lire des objets. Toute autre forme d'accès est refusée.

Si une ACE est vide (qu'elle ne contient aucune lettre du code), aucun droit d'accès n'est accordé.

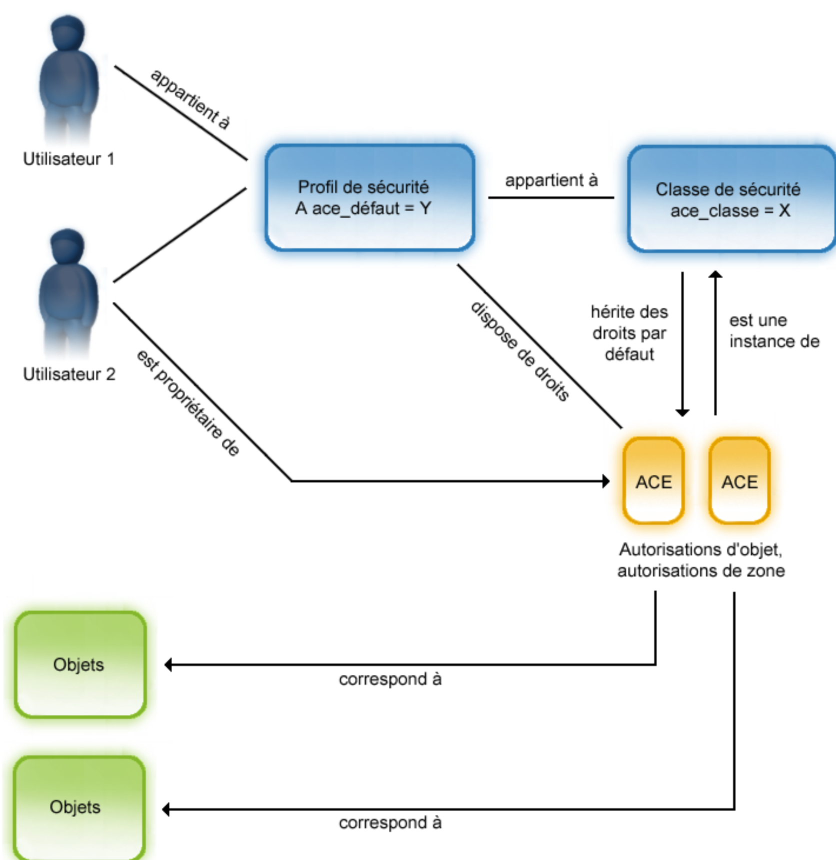
Le tableau suivant définit des autorisations d'objet :

Lettre de code dans une ACE	Signification	Droits accordés
V	Affichage	Permet d'afficher des objets

Lettre de code dans une ACE	Signification	Droits accordés
V	Affichage	Permet d'afficher des objets
C	Créer	Permet de créer des objets
R	Lecture	Permet de lire les sous-objets d'un objet
W	Ecriture	Vous permet de modifier un objet
X	Exécuter	Permet l'exécution, en fonction du type d'objet
D	Supprimer	Permet de supprimer des objets
P	Droit d'accès	Permet de modifier l'ACE même.
O	Ownership	Permet de s'approprier un objet

Un utilisateur appartient à un ou plusieurs profils de sécurité. Un utilisateur peut aussi être le propriétaire d'un objet. Un ensemble de classes de sécurité est affecté à chaque profil de sécurité. Une autorisation de classe de sécurité définit l'autorisation par défaut qui est affectée à un objet, lorsqu'une instance de la classe est créée.

L'illustration ci-dessous indique la manière dont les profils de sécurité, les classes de sécurité et les autorisations d'objet sont liées entre elles et qu'un objet hérite des droits d'une classe de sécurité où l'objet représente une instance de :



Dans l'illustration, l'utilisateur 1 fait partie du profil de sécurité A, l'utilisateur 2 fait partie du profil de sécurité A et est également le propriétaire des objets, représentés par une ACE. Les utilisateurs 1 et 2 disposent de ACE spécifiques, par exemple VR par le biais du profil de sécurité A. L'utilisateur 2 dispose d'une ACE supplémentaire, par exemple VCRWD en tant que propriétaire d'un objet.

Pour vérifier les droits d'accès des utilisateurs 1 et 2 sur un objet, le système de sécurité crée une union (logique) entre l'ACE de l'utilisateur et celle associée à l'objet sécurisé spécifique. Dans l'exemple, les utilisateurs 1 et 2 ont tous les deux des droits d'affichage et de lecture, mais seul l'utilisateur 2 dispose des droits d'écriture et de suppression.

Niveaux de sécurité

Selon la manière dont les autorisations d'objet sont dérivées, il existe différents types de niveaux de sécurité pour l'objet :

Sécurité de niveau de classe

L'autorisation d'objet est dérivée de l'autorisation au niveau de la classe (à partir de la classe à laquelle appartient l'objet) et le niveau de sécurité est défini sur le niveau de la classe. Il s'agit de la valeur par défaut en cas de création d'un objet sécurisé.

Sécurité de niveau de groupe

Lorsqu'un objet sécurisé appartient à un groupe de sécurité où l'héritage est activé, le niveau de sécurité est défini sur le niveau du groupe. Les autorisations sont dérivées du groupe duquel fait partie l'objet (autorisation au niveau du groupe).

Sécurité de niveau d'objet

Lorsque l'utilisateur définit manuellement l'autorisation d'objet pour un objet sécurisé spécifique, le niveau de sécurité est défini sur le niveau de l'objet (en effet, les autorisations sont définies individuellement pour l'objet).

Héritage d'autorisation d'un groupe

Si un objet est membre d'un groupe, le sous-système de sécurité dans Client Automation prend en charge l'héritage dynamique des autorisations à partir d'un groupe vers un membre, comme suit :

- Un indicateur marque un groupe pour un héritage dynamique.
- Tous les membres de ce groupe héritent des autorisations de membre spécifiées.
- Si un membre est ajouté à un groupe, il hérite automatiquement des autorisations du groupe.

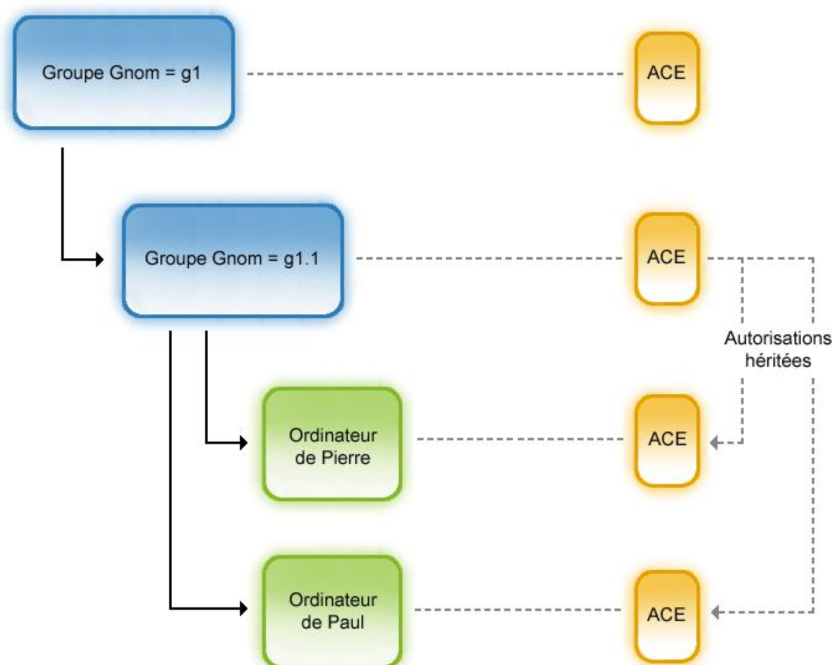
La conception de la sécurité du groupe est basée sur les décisions suivantes :

- L'héritage de la sécurité peut être activé ou désactivé pour un groupe. Lorsqu'il est activé, le groupe devient un groupe de sécurité (l'application peut utiliser une icône différente pour la visualisation).
- Le groupe possède alors deux masques d'autorisation, un pour le groupe même (comme tout autre objet sécurisé) et le masque d'héritage.
- Lorsqu'un groupe hérite d'un groupe parent, les deux masques sont modifiés en fonction du masque d'héritage du groupe parent.
- Le masque d'autorisation d'un membre d'un ou de plusieurs groupes est évalué en fonction de l'union de l'ensemble des autorisations des parents du membre, etc. (les autorisations sont reliées par le connecteur OR).
- L'héritage s'effectue depuis un parent vers un enfant, ce qui peut donner lieu à une mise à jour récursive des objets.
- Il n'existe aucune restriction à la profondeur d'héritage.

- Concernant l'ordre de priorité, les autorisations d'objet sont prioritaires par rapport à celle de groupe, qui sont prioritaires sur les autorisations de classes.
- Si un objet est membre d'un groupe de sécurité au moins, l'unique modification autorisée sur cet objet consiste à appliquer une sécurité d'objet, car l'application d'une sécurité de classe romprait le modèle. Afin que la sécurité de classe devienne active, l'objet doit être supprimé du groupe ou l'héritage de la sécurité doit être désactivée sur le groupe.

Remarque : L'héritage d'un groupe est désactivé si le niveau de sécurité d'un objet est défini sur le niveau de l'objet.

L'illustration suivante indique l'héritage lorsqu'un objet est membre d'un groupe et que ce groupe permet l'héritage des autorisations d'objet :



Le groupe g1.1 est un sous-groupe du groupe g1. Les ordinateurs john et smith sont membres du groupe g1.1.

L'héritage des autorisations est désactivé pour le groupe g1, mais il est activé pour le groupe g1.1. Les ordinateurs john et smith héritent des autorisations du groupe g1.1.

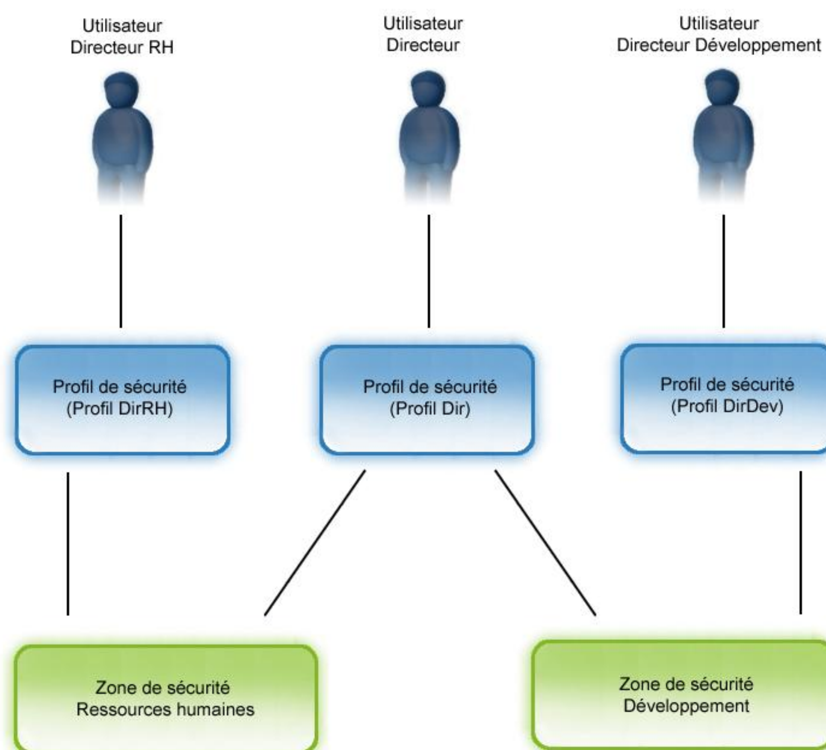
Autorisations pour une zone

Le concept de zone de sécurité étend le modèle de sécurité. Une zone de sécurité constitue une fonctionnalité facultative qui convient aux implémentations importantes avec des milliers d'objets gérés par différents utilisateurs.

Une zone de sécurité constitue une division géographique, organisationnelle ou topologique. La définition de zones de sécurité est utile si vous souhaitez restreindre l'accès des utilisateurs uniquement aux objets liés à leur zone de sécurité. Dans le concept des zones de sécurité, des utilisateurs, représentés par des profils de sécurité, et des objets sont liés à des zones de sécurité. Une zone de sécurité peut être liée à un ou plusieurs profils et à un ou plusieurs objets. Un utilisateur peut accéder à un objet si l'une des zones de sécurité au moins liée à l'objet l'est également au moins à un profil de sécurité de l'utilisateur. Si l'accès à l'objet est refusé, l'objet n'est pas visible pour l'utilisateur.

Exemple : Deux zones de sécurité et trois utilisateurs

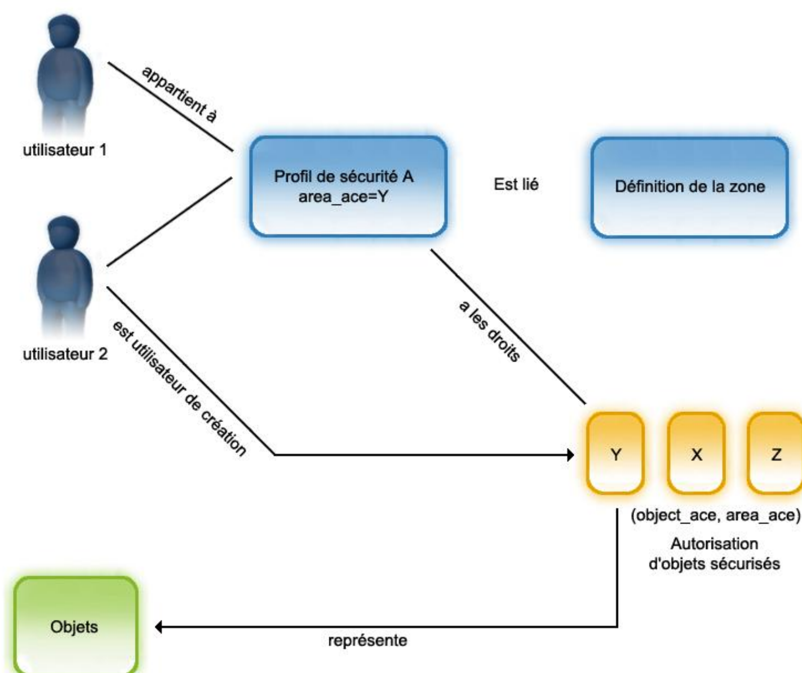
Trois profils utilisateurs (HRMgrProfile, SrMgrProfile et DevMgrProfile, avec tous les droits d'accès) ont été assignés à trois utilisateurs (HRManager, SeniorManager et DevManager). Deux zones de sécurité ont été définies, HumanResources et Development. Les profils HRMgrProfile et SrMgrProfile sont reliés à la zone de sécurité HumanResources. Les profils SrMgrProfile et DevMgrProfile sont reliés à la zone de sécurité Development. Puis SeniorManager, représenté par le profil SrMgrProfile, a accès aux deux zones, HumanResources et Development. HRManager dispose uniquement des droits d'accès à la zone de sécurité HumanResources et DevManager uniquement à la zone Development. Par exemple, si HRManager crée une requête sur sa console dans la zone HumanResources, DevManager ne la voit pas. Seuls les objets créés par le système sont visibles pour tous les profils utilisateur.



La définition des autorisations de zone permet de limiter les droits d'accès sur un objet particulier d'un ou de plusieurs profils. Cela signifie que même les autorisations au niveau de la classe définies pour un profil sont identiques. Vous pouvez affecter ou lier un objet à différentes zones ou restreindre l'accès pour des profils, afin d'afficher uniquement les objets liés à une zone spécifique.

En plus des autorisations d'objet, qui sont gérées par les classes de sécurité, le sous-système de sécurité permet de créer jusqu'à 32 zones.

L'illustration suivante fournit un aperçu de la prise en charge de zone du sous-système de sécurité.



Les utilisateurs 1 et 2 font partie du profil de sécurité A. Dans la définition de la zone reliée au profil A, sont indiquées les zones visibles par les utilisateurs faisant partie du profil A.

L'utilisateur 2 a créé un objet visible par tous les utilisateurs reliés à la zone concernée.

Pour les cas d'utilisation importante et les descriptions des opérations effectuées par la prise en charge de zone dans ces cas d'utilisation, reportez-vous à la section Cas d'utilisation de prise en charge des zones de sécurité (page 589).

Conditions préalables à l'accès aux objets dans les différentes zones

Les conditions suivantes doivent être remplies avant l'évaluation de l'autorisation de zone de l'utilisateur :

- L'utilisateur doit disposer d'un accès à l'objet (affichage ou lecture).
- La prise en charge des zones de sécurité sur le gestionnaire de domaines doit être activée.
- Tous les profils de sécurité dont l'utilisateur est membre doivent être activés pour la prise en charge des zones de sécurité.

Si la première condition n'est pas remplie, l'accès à l'objet est refusé à l'utilisateur, quelles que soient la deuxième et la troisième conditions. Si la deuxième ou la troisième condition n'est pas remplie, l'utilisateur n'est pas restreint en fonction des autorisations de zone et peut accéder à tous les objets.

Remarques :

- Tous les objets sont accessibles aux utilisateurs membres de profils de sécurité dont la zone de sécurité est désactivée. Nous recommandons à l'administrateur de s'assurer que tous les profils de sécurité soient activés pour la prise en charge des zones de sécurité.
- La prise en charge des zones de sécurité n'est pas disponible sur les gestionnaires d'entreprise DSM.
- Le profil Distributions constitue l'unique profil intégré pouvant être activé pour la prise en charge des zones de sécurité. Tous les autres profils intégrés sont désactivés pour la prise en charge des zones de sécurité.
- Les objets qui appartiennent aux classes de sécurité "Procédure" ou "Job logiciel" ne peuvent pas être liés à une zone de sécurité dans l'explorateur DSM. Ils sont automatiquement liés aux zones auxquelles sont liés leurs conteneurs parents (Package logiciel et Conteneur de jobs logiciels).

Autorisations dérivées pour une zone

Les autorisations concernant une zone peuvent être définies ou dérivées de plusieurs manières :

Autorisation de zone du profil de sécurité

Si l'utilisateur de création est valide lors de la création d'un objet sécurisé, alors les autorisations de zone sont dérivées de l'utilisateur ayant créé l'objet.

(niveau de sécurité : Utilisateur de création)

Autorisation de zone d'un groupe

Ce cas s'applique uniquement lorsque l'objet sécurisé est membre d'un groupe et que l'héritage est activé.

(niveau de sécurité : Groupe)

Autorisation de zone définie manuellement

Un utilisateur peut définir manuellement l'autorisation de zone pour un objet spécifique.

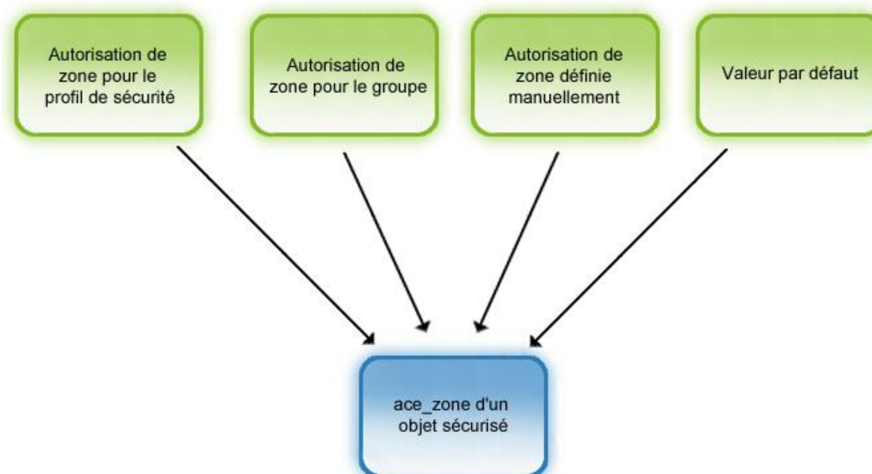
(niveau de sécurité : Objet)

Autorisation de zone par défaut

Si un objet sécurisé est créé et que l'utilisateur de création n'est pas défini ou est introuvable dans la liste d'utilisateurs, alors les autorisations de zone proviennent des paramètres de configuration globaux (autorisations globales par défaut).

(niveau de sécurité : Paramètres globaux)

L'illustration suivante indique les différentes manière de dériver une autorisation de zone :



Réplication

Le sous-système de sécurité exclut les données d'autorisation de la réplication entre les niveaux entreprise et domaine. Le nombre important d'objets détenant les données d'autorisation les rend inadaptés à la réplication. Au lieu de cela, la sécurité est réinitialisée pour un objet déplacé d'une base de données vers une autre.

Cela signifie que les autorisations (autorisations d'objet et de zone) doivent être recalculées dès la création d'un objet sécurisé répliqué. Cela s'applique aussi bien à la réplication ascendante qu'à la réplication descendante. La réplication de Définitions de zone, par exemple, n'est pas requise.

- **Pré-conditions**
  - Une requête est créée au niveau de l'entreprise par un utilisateur X.
  - L'utilisateur X dispose uniquement d'un accès aux zones 1 et 2.
  - L'utilisateur X est également connu au niveau du domaine et dispose d'un accès à la zone 5 uniquement.
- **Action**

  Une requête est dupliquée de manière descendante.
- **Post-conditions**
  - Une requête est créée au niveau du domaine.
  - L'autorisation de zone est paramétrée comme défini par l'utilisateur de création, dans ce cas, pour l'utilisateur X.
  - L'utilisateur X au niveau du domaine ne peut apercevoir la requête, car l'utilisateur ne dispose pas d'autorisations de zone pour les zones 1 et 2.

Limites

- Les tâches Software Delivery sont toujours visibles dans le Panneau de configuration pour tous les administrateurs, car ces tâches ne sont pas sécurisées (ni les autorisations d'objets ou de zone). Toutefois la liste des tâches est en lecture seule.
- Les autorisations pour les objets d'application Software Delivery proviennent de l'objet cible.
- Le nombre de zones est limité à 32.

Scénario de sécurité - Software Delivery

Le scénario suivant vous permet de mieux comprendre le concept de sécurité.

Scénario :

Vous souhaitez permettre à un utilisateur de créer un logiciel et d'avoir toutes les autorisations pour modifier et distribuer ce logiciel à un groupe précis d'ordinateurs. En même temps, vous voulez refuser ces autorisations à d'autres utilisateurs.

Vous pouvez créer plusieurs groupes d'utilisateurs, afin de créer des îlots de sous-administrateurs indépendants.

Ouvrir la boîte de dialogue Profils de sécurité. N'apportez pas de modification aux groupes Tout le monde et Propriétaire/créateur et vous pouvez réserver le groupe d'administrateurs aux utilisateurs disposant d'avantage de privilèges. Vous devez donc définir de nouveaux profils de sécurité pour ce scénario.

Pour implémenter le scénario ci-dessus

1. Créez un nouveau profil de sécurité, UTILISATEUR1 (compte utilisateur), devant disposer d'une utilisation restreinte.
2. Définissez les autorisations de classes pour ce profil, comme illustré dans le tableau suivant, à l'aide du groupe Administrateur :

Classe d'objet	Autorisations de classes	Commentaires
Package logiciel	Accès spécial (C)	Crée le package logiciel. Aucun autre droit n'est requis si vous être propriétaire du package logiciel après l'avoir créé.
Procédure	Accès spécial (C)	Crée une procédure.
Job logiciel	Accès spécial (C)	Crée un job logiciel sur l'ordinateur cible.
Conteneur de jobs logiciels	Accès spécial (CVRW)	Crée, écrit et affiche le conteneur de jobs. Accès disponible dans le dossier Jobs, Jobs logiciels, Tous les jobs logiciels.

Classe d'objet	Autorisations de classes	Commentaires
Package logiciel	Accès spécial (C)	Crée le package logiciel. Aucun autre droit n'est requis si vous être propriétaire du package logiciel après l'avoir créé.
Accès prioritaire du conteneur de jobs	Aucun accès	Empêche l'utilisateur de modifier la priorité du conteneur de jobs. **Remarque :** Les conteneurs de jobs de priorité élevée forcent le gestionnaire de tâches à retarder l'exécution des conteneurs de jobs de faible priorité.
Toutes les autres classes d'objets	Aucun accès	Restreint l'accès de l'utilisateur aux autres objets.

3. Accédez au groupe d'actifs sur lequel vous souhaitez distribuer le logiciel et définissez les autorisations du groupe pour ce profil comme suit :

   - Accès à l'objet : Gérer (VRX)
   - Accès aux membres : Gérer (VRX)

   Remarque : Le groupe d'actifs spécifique doit être un groupe de sécurité avec l'option Les membres héritent des autorisations.

4. Définissez les autorisations de lecture (VR) pour les objets (Nœud de) Domaine, Ordinateur et Bibliothèque de packages logiciels dans la boîte de dialogue Autorisations d'objet.

L'utilisateur ne peut afficher que les jobs qu'il a créés.

Définissez un autre profil de sécurité similaire, UTILISATEUR2. UTILISATEUR2 n'aura pas accès à l'ordinateur, aux groupes de logiciels et aux jobs d'UTILISATEUR1, et inversement.

Si UTILISATEUR1 observe les installations sur les ordinateurs du groupe Spécial, les installations commandées sont visibles. De même, le logiciel Software Delivery installé sur ces ordinateurs est visible pour UTILISATEUR1 à cet emplacement et à aucun autre.

Configuration de la sécurité commune

La configuration de la sécurité est l'une des étapes cruciales suivant l'installation, car elle fournit la passerelle vers le système CA Client Automation. Vous pouvez décider du modèle de sécurité qui convient à votre organisation et configurer le système de sécurité en conséquence. La décision concernant le modèle de sécurité peut être effectuée sur la base des facteurs suivants :

- Utilisateurs individuels et groupes (à la fois locaux et de domaine) ayant besoin d'accéder au système.
- Le type d'accès (lire, écrire, exécuter, etc.) requis par chaque utilisateur et chaque groupe.
- Le niveau d'autorisation requis : autorisations de classes, de groupe ou de niveau de zone.

Remarque : Si un utilisateur dispose de deux profils, l'un mappé sur son compte utilisateur et l'autre mappé sur un groupe, les autorisations en résultant représentent l'union des autorisations des deux profils. Cette règle est également valide si un utilisateur est membre de plusieurs groupes définis en tant que profils de sécurité.

Par défaut, un contrôle d'accès total est accordé aux membres du groupe d'administrateurs. Ainsi, une fois l'installation de CA Client Automation achevée, tous les membres du groupe d'administrateurs peuvent se connecter au domaine DSM, créer des utilisateurs supplémentaires et accorder des droits d'accès.

Configuration de la sécurité

La configuration de l'accès sécurisé contrôlé au système implique les tâches suivantes. La compréhension de ces tâches vous aide à définir un système de sécurité puissant et efficace.

- Ajout de profils de sécurité au système. Par défaut, les profils prédéfinis sont ajoutés au système de sécurité et ne peuvent pas être supprimés.
- Spécification des autorisations de classes pour les classes d'objets répertoriées dans la boîte de dialogue Autorisations de classes.

  Assurez-vous d'interdire aux profils de modifier les droits d'accès aux classes d'objets de profils de sécurité, de zones de sécurité et d'autorisations de classes. Ouvrez les profils et définissez leur type d'accès d'autorisation de classe sur Aucun accès pour ces trois classes d'objets.

Cependant, pour ajuster au mieux le système de sécurité, vous pouvez procéder comme suit :

- Définir l'accès du groupe ou de l'objet pour chaque dossier ou objet visible dans l'Explorateur.
- Utiliser un accès spécial pour sélectionner une combinaison de permissions d'accès : visualiser, lire, écrire, supprimer, exécuter, modifier les autorisations et s'approprier.

Tout utilisateur de système d'exploitation disposant d'un compte valide sur le gestionnaire de domaines peut se connecter au système. Cet utilisateur n'a plus besoin d'être administrateur. L'accès aux fonctionnalités et fonctions système est contrôlé par ses mécanismes de sécurité internes. Par défaut, les administrateurs et le propriétaire jouissent d'un accès total, toutes les autres personnes ne disposant d'aucun accès. Cependant, vous pouvez modifier les droits d'accès en mettant à jour les autorisations après l'installation.

Remarque : Si vous êtes connecté au gestionnaire d'entreprise, assurez-vous de posséder un compte disposant de droits d'utilisateur (ou droits de groupe d'utilisateurs) suffisants pour accéder aux fonctions de sécurité sur chaque gestionnaire de domaine en aval. Si vous êtes connecté à un gestionnaire de domaines, assurez-vous de posséder un compte doté de droits suffisants pour accéder aux fonctions de sécurité sur le gestionnaire d'entreprise.

Ajout de profil de sécurité

La création d'un profil de sécurité signifie en mapper un nouveau sur un compte utilisateur ou un groupe proposé par les fournisseurs de sécurité actuels. Vous pouvez sélectionner les utilisateurs ou les groupes qui peuvent accéder au système et les ajouter à un profil de sécurité.

Pour ajouter des profils de sécurité

1. Sélectionnez des profils de sécurité à partir du menu Sécurité.

   La boîte de dialogue Profils de sécurité s'affiche.

   Remarque : Vous devez disposer des droits d'accès permettant d'ouvrir cette boîte de dialogue ; sinon, un message d'erreur de sécurité apparaît. Les administrateurs disposent de ces droits d'accès par défaut.

2. Cliquez sur Ajouter.

   La boîte de dialogue Ajouter des profils de sécurité apparaît.

3. Sélectionnez l'autorité de sécurité à partir de l'arborescence des répertoires disponibles, parcourez et cliquez sur l'entité de sécurité requise.

   Vous pouvez afficher l'autorité et l'entité de sécurité sélectionnées respectivement dans l'identificateur de conteneur et les champs Noms.

4. Double-cliquez sur une entité dans l'arborescence ou cliquez sur Ajouter à la liste.

   Les entités de sécurité qui apparaissent dans le champ Noms sont ajoutées à la liste des profils de sécurité.

   Pour ajouter plus de profils, répétez les deux dernières étapes dans la boîte de dialogue Ajouter des profils de sécurité.

5. Cliquez sur OK.

   Le compte ou le groupe d'utilisateurs sélectionné est mappé au profil de sécurité et la boîte de dialogue Autorisations de classes est affichée.

   Remarque : Si vous avez ajouté plusieurs entités de sécurité, la boîte de dialogue Autorisations de classe n'est pas affichée. Vous devez sélectionner le profil dans la boîte de dialogue Profils de sécurité et cliquer sur Autorisations de classes.

6. Dans la boîte de dialogue Autorisations de classes, sélectionnez la classe d'objet à laquelle vous souhaitez attribuer les droits.

   Remarque : Vous pouvez sélectionner plusieurs classes d'objets et spécifier les autorisations de classes pour tous. Pour une sélection continue, appuyez sur la touche Maj et cliquez sur les objets ; pour une sélection aléatoire, appuyez sur la touche Ctrl et cliquez sur les objets.

7. Sélectionnez l'autorisation dans la liste déroulante d'accès aux classes et cliquez sur OK.

   Les autorisations accordées sont affectées au nouveau profil de sécurité.

La boîte de dialogue Ajout de profils de sécurité affiche une liste des autorités de sécurité disponibles : les domaines Windows NT, les cibles d'authentification UNIX, les répertoires externes tels que NDS et LDAP et le sous-système de certificat X.509.

Cette liste d'autorités de sécurité disponibles est stockée dans le gestionnaire. Lors de l'exécution dans un environnement de domaine Windows NT, le noeud du gestionnaire calcule automatiquement toutes les approbations de domaine explicites disponibles. Celles-ci sont renvoyées pour un affichage lorsque la liste des autorités disponibles est requise par la boîte de dialogue Ajouter des profils de sécurité.

Dans certains cas, vous souhaitez utiliser un domaine approuvé implicitement lors de la création de profils de sécurité, un domaine qui ne se trouve pas directement dans la liste calculée. Pour activer cela, la boîte de dialogue Profils de sécurité vous permet d'ajouter et de supprimer des autorités, mais uniquement dans l'espace de nom Windows NT (winnt).

Pour ajouter un domaine approuvé implicitement, cliquez sur Ajouter et entrez le nom de domaine dans la nouvelle boîte de dialogue. Une fois que vous avez cliqué sur OK, le domaine est ajouté à la liste des autorités disponibles. Pour supprimer un domaine approuvé implicitement, sélectionnez ce domaine et cliquez sur Supprimer.

L'ajout d'un domaine à la liste d'autorités ne lui confère aucune approbation ; cela est renforcé par le système d'exploitation. Il n'est pas possible d'ajouter un domaine à cette liste et que ce domaine soit approuvé par le gestionnaire, sauf si le système d'exploitation approuve déjà le domaine en question.

Types d'accès prédéfinis

Les types d'accès indiquent les droits d'accès à un objet ou à un dossier. Un type d'accès prend l'une des valeurs suivantes :

Afficher

Autorisations d'afficher (V)

Lecture

Autorisations d'afficher et de lire (VR)

Gérer

Autorisations d'afficher, de lire et d'exécuter (VRX)

Changement

Autorisations d'afficher, de lire, d'écrire, d'exécuter et de supprimer (VRWXD)

Contrôle absolu

Autorisations de créer, afficher, lire, écrire, exécuter, supprimer, modifier les autorisations et s'approprier (CVRWXDPO)

Accès spécial

Si vous souhaitez bénéficier d'une autre combinaison de droits, sélectionnez Accès spécial. La boîte de dialogue Accès spécial s'affiche avec tous les droits.

Aucun accès

Empêche l'utilisateur d'accéder aux objets dans la classe d'objet.

Remarque : N'attribuez pas cette valeur au groupe Propriétaire / Créateur. Elle pourrait bloquer complètement l'accès à l'application.

L'exemple suivant décrit les résultats de différents droits d'accès sur la classe d'objet Ordinateur :

Accès aux classes	Autorisation résultante
Afficher	Affiche tous les ordinateurs dans le dossier Tous les ordinateurs.
Lecture	Vous permet d'afficher les propriétés des ordinateurs.
Gérer	Vous permet de déployer un package logiciel ou d'exécuter un job sur un ordinateur.
Changement	Vous permet d'ajouter un nouvel ordinateur ou de supprimer un ordinateur.
Contrôle absolu	Vous octroie le contrôle absolu sur les ordinateurs.

Spécifier les autorisations de classes

Vous pouvez modifier les autorisations de classes attribuées à un profil de sécurité.

Pour spécifier des autorisations de classes

1. Sélectionnez Profils de sécurité dans le menu Sécurité.

   La boîte de dialogue Profils de sécurité s'affiche.

2. Sélectionnez le profil de sécurité pour lequel vous souhaitez modifier les autorisations de classes et cliquez sur Autorisations de classes.

   La boîte de dialogue Autorisations de classes s'affiche.

3. Sélectionnez la classe d'objet à laquelle vous devez attribuer les droits.

   Remarque : Vous pouvez sélectionner plusieurs classes d'objets et spécifier les autorisations de classes pour tous. Pour une sélection continue, appuyez sur la touche Maj et cliquez sur les objets ; pour une sélection aléatoire, appuyez sur la touche Ctrl et cliquez sur les objets.

4. Sélectionnez les autorisations de classes dans le champ Accès aux classes et cliquez sur OK.

   Les membres du profil de sécurité sélectionné peuvent maintenant accéder à la classe d'objet jusqu'au niveau spécifié.

   Pour spécifier différentes combinaisons de droits, sélectionnez Accès spécial dans cette liste déroulante d'accès à un objet.

Spécifier des autorisations d'objet

Vous pouvez spécifier des autorisations d'objet pour chaque objet, comme un ordinateur, un utilisateur, un job, etc. Par défaut, un objet hérite des autorisations de classes provenant de sa classe d'objet.

Remarque : Les autorisations sur les objets sont prioritaires par rapport aux autorisations sur les classes et de groupe.

Pour spécifier des autorisations d'objet

1. Sélectionnez les objets et utilisez l'une des méthodes suivantes :
   - Sélectionnez Autorisations dans le menu Sécurité.
   - Cliquez avec le bouton droit de la souris sur l'objet, puis sélectionnez Autorisations dans le menu contextuel.

   La boîte de dialogue Autorisations d'objet s'affiche.

   Remarque : Vous pouvez sélectionner plusieurs classes d'objets et spécifier les autorisations de classes pour tous. Pour une sélection continue, appuyez sur la touche Maj et cliquez sur les objets ; pour une sélection aléatoire, appuyez sur la touche Ctrl et cliquez sur les objets.
2. Sélectionnez le type d'accès requis à partir de la liste déroulante Accès à l'objet et cliquez sur OK.

   Les membres du profil peuvent accéder à l'objet avec les droits qui leur ont été accordés.

   Pour spécifier différentes combinaisons de droits, sélectionnez Accès spécial dans cette liste déroulante d'accès à un objet.

Spécifier les autorisations de groupe

Des autorisations de groupe peuvent être spécifiées pour tous les dossiers créés par l'utilisateur.

Remarque : Concernant l'ordre de priorité, les autorisations d'objet sont prioritaires par rapport à celles de groupe, qui sont prioritaires sur les autorisations de classes. Cela signifie que la définition d'autorisations de classes ne remplace pas les autorisations d'objet et de membres de groupe spécifiées individuellement.

Pour spécifier des autorisations de groupe

1. Sélectionnez le dossier et utilisez l'une des méthodes suivantes :
   - Sélectionnez Autorisations dans le menu Sécurité.
   - Cliquez avec le bouton droit de la souris sur le groupe, puis sélectionnez Autorisations dans le menu contextuel.

   La boîte de dialogue Autorisations du groupe de sécurité s'affiche et vous permet de définir les autorisations au niveau du groupe.
2. Sélectionnez un profil et spécifiez l'accès à l'objet et l'accès au membre.

   Remarque : Sélectionner la valeur par défaut permet de remplacer les autorisations de membre par les autorisations de classe.

   Les membres du profil peuvent maintenant accéder au dossier ou au groupe jusqu'au niveau spécifié.

   Pour spécifier différentes combinaisons de droits, sélectionnez Accès spécial dans cette liste déroulante d'accès à un objet.

Autorisations cumulées

Les autorisations sont toujours cumulées pour les profils de sécurité mappés, comme expliqué dans les instructions et exemples suivants :

- Si un utilisateur est membre de plusieurs groupes de sécurité, les droits de chaque groupe sont reliés par l'opérateur OR pour déterminer les droits d'accès de cet utilisateur.

  Par exemple, si un utilisateur est membre de deux groupes et si l'un des groupes dispose d'un accès en écriture pour un objet et l'autre groupe bénéficie d'un accès en lecture, l'utilisateur peut alors disposer de l'accès en écriture.
- les autorisations au niveau de l'objet remplacent les autorisations au niveau du groupe, qui remplacent quant à elles les autorisations au niveau de la classe.

Exemples :

- Pour développer un dossier (par exemple, afin d'afficher la liste des ordinateurs d'un groupe), vous devez disposer des droits de lecture sur ce dossier.
- Pour créer un objet, vous devez disposer des droits de création pour cet objet.

  Si l'objet créé doit être placé dans un dossier, vous devez également disposer des droits de lecture et d'écriture sur ce dossier.
- Les opérations de collage et de liaison nécessitent des droits d'écriture sur le dossier ou l'objet en cours (par exemple, lorsque l'utilisateur colle des fichiers et des dossiers).
- L'opération de déplacement nécessite des droits d'écriture sur deux dossiers ou objets, le dossier source et celui de destination.

Prise en charge de la zone de sécurité

Une zone de sécurité constitue une division géographique, organisationnelle ou topologique. Une zone de sécurité peut être liée à un ou plusieurs profils de sécurité et à un ou plusieurs objets. Un utilisateur peut accéder à un objet si au moins l'une des zones de sécurité liée à l'objet l'est également à au moins un profil de sécurité de l'utilisateur.

Pour vous documenter sur les cas importants d'utilisation de la prise en charge des zones en contexte, reportez-vous à la section Cas d'utilisation de la prise en charge des zones de sécurité (page 589).

Dans les sections ci-dessous, vous trouverez des informations sur l'utilisation de ces zones de sécurité.

Paramètres globaux des zones de sécurité

Les paramètres globaux définissent l'état de la prise en charge des zones de sécurité, et déterminent si les objets créés par le système sont affichés ou masqués dans la zone de sécurité. Vous pouvez modifier les paramètres globaux dans la boîte de dialogue Zones de sécurité, disponible à partir du menu Sécurité.

La prise en charge des zones de sécurité au niveau du gestionnaire de domaines est désactivée par défaut. Vous devez l'activer pour implémenter la fonctionnalité de zone de sécurité dans votre système de sécurité, même si vous pouvez créer et lier des zones à des profils et des objets sans activer cette option. Pour activer la prise en charge des zones de sécurité au niveau du gestionnaire de domaines, sélectionnez le bouton d'option d'activation du champ Prise en charge de la zone de sécurité.

Par défaut, les zones de sécurité sont configurées pour afficher les objets créés par le système. Si vous voulez masquer ces objets dans une zone de sécurité spécifique, désactivez la case à cocher en regard du nom de la zone de sécurité dans la boîte de dialogue Zones de sécurité.

Activation d'un paramètre de zone de sécurité pour un profil de sécurité

Vous devez activer la prise en charge de zone de sécurité pour chaque profil de sécurité adapté, afin d'implémenter cette fonctionnalité au niveau du profil de sécurité.

Pour activer un paramètre de zone de sécurité pour un profil de sécurité

1. Sélectionnez des profils de sécurité à partir du menu Sécurité.

   La boîte de dialogue Profils de sécurité s'affiche.

2. Sélectionnez les profils de sécurité pour lesquels vous voulez activer des paramètres de zone de sécurité, puis cliquez sur Zones de sécurité.

   La boîte de dialogue Liaisons des zones de sécurité s'affiche.

3. Cochez la case Activer la prise en charge des zones de sécurité pour ce profil.

   L'icône située en regard de la case à cocher affiche une coche verte, afin d'indiquer que la prise en charge de la zone de sécurité est activée.

Création d'une zone de sécurité

Vous pouvez créer des zones pour chaque division géographique, topologique ou organisationnelle ou tout autre type de gestion de zone de votre choix.

Pour créer une zone de sécurité

1. Sélectionnez des zones de sécurité à partir du menu Sécurité.

   La boîte de dialogue Zones de sécurité s'affiche.

2. Cliquez sur Ajouter.

   La boîte de dialogue Nouvelle zone de sécurité s'affiche.

3. Entrez un nom et une description pour la nouvelle zone, puis cliquez sur OK.

   La nouvelle zone est ajoutée à la liste de zones de sécurité dans la boîte de dialogue Zones de sécurité et la boîte de dialogue Liaisons de profils de sécurité s'affiche, à partir de laquelle vous vous lier des profils de sécurité à la nouvelle zone.

Suppression d'une zone de sécurité

Vous pouvez supprimer une zone de sécurité dont vous n'avez plus besoin. Une zone de sécurité supprimée est retirée du système et sa liaison est automatiquement supprimée à partir de tous les profils et objets liés.

Pour supprimer une zone de sécurité

1. Sélectionnez des zones de sécurité à partir du menu Sécurité.

   La boîte de dialogue Zones de sécurité s'affiche.

2. Cliquez sur Supprimer.

   Un message de confirmation apparaît.

3. Cliquez sur Oui.

   La zone de sécurité est supprimée.

Liaison ou suppression de liaison d'une zone de sécurité vers ou à partir de profils de sécurité

La liaison d'un profil de sécurité avec une zone de sécurité permet aux utilisateurs ou aux groupes d'accéder uniquement à ces objets liés à leurs zones de sécurité. Vous pouvez lier un profil de sécurité à une ou plusieurs zones de sécurité adaptées. Dans le cas de plusieurs zones, les utilisateurs disposent d'un accès aux objets liés à l'ensemble des zones de sécurité auxquelles ils appartiennent.

Vous pouvez supprimer une liaison de zone de sécurité si l'utilisateur n'appartient plus à cette zone.

Pour lier ou supprimer une liaison de zones de sécurité

1. Sélectionnez des profils de sécurité à partir du menu Sécurité.

   La boîte de dialogue Profils de sécurité s'affiche.

2. Sélectionnez les profils de sécurité et cliquez sur Zones de sécurité

   La boîte de dialogue Liaisons des zones de sécurité s'affiche et répertorie l'état de liaison des profils sélectionnés.

3. Sélectionnez les zones de sécurité et cliquez sur Lier ou Supprimer la liaison

   Les profils de sécurité sélectionnés sont liés avec les zones de sécurité ou leur liaison avec celles-ci est supprimée.

Liaison ou suppression de liaison d'une zone de sécurité vers ou à partir d'objets sécurisés

La liaison d'un objet sécurisé avec une zone de sécurité permet uniquement aux utilisateurs appartenant à cette zone d'accéder à l'objet. Vous pouvez lier un objet sécurisé à une ou plusieurs zones adaptées. Dans le cas de plusieurs zones, l'objet devient accessible aux utilisateurs liés à l'ensemble des zones de sécurité auxquelles l'objet appartient.

Remarque : Lorsque vous créez ou supprimez la liaison d'un objet vers ou depuis un groupe, l'objet hérite automatiquement des autorisations de zone du groupe, que les autorisations de zone soient définies ou non pour cet objet. Si vous voulez conserver les autorisations de zone au niveau de l'objet, vous devez réviser et modifier les autorisations de zone après la création ou la suppression de la liaison de l'objet.

Pour lier ou supprimer une liaison de zones de sécurité

1. Sélectionnez les objets dans l'Explorateur et cliquez avec le bouton droit de la souris.

   Le menu contextuel s'affiche.

2. Sélectionnez Autorisations.

   La boîte de dialogue Autorisations d'objet s'affiche.

3. Cliquez sur Zones de sécurité.

   La boîte de dialogue Liaisons des zones de sécurité s'affiche et répertorie l'état de liaison des objets sélectionnés.

4. Sélectionnez les zones de sécurité et cliquez sur Lier ou Supprimer la liaison

   Les objets sécurisés sélectionnés sont liés avec les zones de sécurité ou leur liaison avec celles-ci est supprimée.

Configuration du chiffrement

Client Automation fournit une prise en charge pour les algorithmes de chiffrement plus forts, en particulier pour l'algorithme AES (Advanced Encryption Standard), au sein du sous-système de la messagerie de session et des composants directement associés.

Vous pouvez configurer les algorithmes de chiffrement utilisés pour la communication avec d'autres partenaires à l'aide de stratégies de chiffrement. Cette configuration est valide pour la communication à l'aide de la messagerie de session, la fonction stocker et transférer de Software Delivery, la communication visionneuse/hôte de Remote Control, l'agent DTS et le serveur Software Delivery pour le transfert de fichier non-NOS.

Les algorithmes de chiffrement disponibles, la sélection du meilleur algorithme pour la communication et la communication avec des partenaires antérieurs à r11.2 sont pris en compte dans les sections suivantes :

- Algorithmes de chiffrement pour la communication (page 450)
- Méthode de choix de l'algorithme de chiffrement correspondant (page 450)
- Chiffrement dans des environnements top secret (page 451)
- Communication avec des versions antérieures (page 452)

Algorithmes de chiffrement pour la communication

Les algorithmes de chiffrement utilisés pour la communication et leur ordre favori sont définis dans une stratégie de chiffrement, la liste de préférences de chiffre.

Lorsqu'une communication doit être établie, les algorithmes définis des deux partenaires de communication sont pris en compte et l'algorithme favori de la liste est choisi pour la session qui suit. Pour établir une session de communication, un algorithme commun au moins doit être partagé par les deux partenaires de communication.

La liste suivante affiche les algorithmes de chiffrement disponibles, triés par l'ordre croissant de leur force (AES-256 est donc le plus fort) :

Triple-DES (Data Encryption Standard)

Indique une clé symétrique, selon l'algorithme Data Encryption Standard avec une longueur de clé de 168 bits.

AES-128 (Advanced Encryption Standard)

Indique une clé symétrique, selon l'algorithme Advanced Encryption Standard avec une longueur de clé de 128 bits.

AES-192

Indique une clé symétrique, selon l'algorithme Advanced Encryption Standard avec une longueur de clé de 192 bits.

AES-256

Indique une clé symétrique, selon l'algorithme Advanced Encryption Standard avec une longueur de clé de 256 bits.

Sélection de l'algorithme de chiffrement correspondant

Chaque partenaire de communication comprend une liste de chiffrements préférés définis dans la politique de chiffrement, le chiffrement préféré sur tous les autres étant défini en premier dans la liste. Les listes des deux partenaires de communication sont comparées et évaluées selon les règles suivantes :

- Pour chaque liste, les chiffrements sont considérés dans leur totalité et un chiffrement correspondant est recherché dans l'autre liste jusqu'à ce qu'il y ait une correspondance ou que la liste se termine.
- Si deux chiffrements correspondants sont renvoyés, le chiffrement le plus fort est utilisé pour la session suivante.
- S'il y a uniquement un chiffrement correspondant, ce chiffrement est utilisé pendant la session suivante.
- Si aucun chiffrement correspondant n'a été trouvé, les communications ne sont pas possibles.

Exemple :

La liste de chiffrements du partenaire A contient : Triple-DES, AES-192 et AES-128. La liste de chiffrements du partenaire B contient : AES-256, AES-128, Triple-DES et AES-192.

Le système effectue les opérations suivantes pour identifier des chiffrements correspondants :

1. Vérifiez la liste de chiffrements du partenaire A :

   La première entrée, Triple-DES, est recherchée dans la liste du partenaire B.

   Une correspondance est renvoyée et Triple-DES est le premier chiffrement correspondant.

2. Vérifiez la liste de chiffrements du partenaire B :

   La première entrée, AES-256, est recherchée dans la liste du partenaire A.

   Aucune correspondance n'est renvoyée.

   La seconde entrée, AES-128, est recherchée dans la liste du partenaire A.

   Une correspondance est renvoyée et AES-128 est le second chiffrement correspondant.

3. Le système considère que le chiffrement AES-128 est plus fort que le chiffrement Triple-DES et utilise cet algorithme pour la session suivante.

Remarque : Seules les deux premières correspondances sont considérées. Aucune autre recherche n'est effectuée dans les deux listes de chiffrement.

Chiffrement dans des environnements top secret

Pour les clients devant utiliser le chiffrement dans leur environnement top secret, nous conseillons d'installer en premier le gestionnaire, puis de modifier la stratégie par défaut pour les préférences du chiffre afin que AES-256 soit le seul élément de la liste et de définir la propriété DSM/common components/encryption/compatibility/pre_11_2 sur Faux.

Dès que la modification de la configuration est effectuée pour l'agent sur le système du gestionnaire (le job de configuration est terminé), vous pouvez installer des serveurs de modularité supplémentaires en toute sécurité.

Au niveau du serveur de modularité, vous devez vérifier si la liste des chiffres s'est étendue en entrant les commandes :

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences -pncipher0
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences -pncipher1
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences -pncipher2
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences –pncipher3
```

Le chiffre 0 doit contenir AES-256 et les autres chiffres doivent être vides. Cette opération peut être réalisée au niveau du gestionnaire ou de l'agent pour vérifier si la configuration du chiffre est déjà effectuée.

Vous pouvez alors installer en toute sécurité des agents pointant vers ce serveur. Les agents utilisent immédiatement le chiffrement AES-256 pour communiquer.

Dès que la configuration commune est appliquée aux agents, AES-256 est également le seul élément de leur liste de chiffres et les agents ne parviennent pas à communiquer lorsqu'ils sont contactés avec un autre chiffre.

Communication avec des versions antérieures (stratégie Compatibility)

Pour communiquer avec des partenaires antérieurs à la version r11.2, la stratégie de compatibilité préalable à la version 11.2 doit être définie sur True (Vrai).

Avec la configuration par défaut, cette valeur de stratégie est définie.

Lorsqu'il ne reste plus d'installations antérieures à la version 11.2 dans tout l'environnement, vous devez définir la stratégie de compatibilité pre_11_2 sur False (Faux) pour améliorer l'établissement d'une session.

Cryptographie conforme à la norme FIPS

Client Automation prend en charge la cryptographie conforme à la norme FIPS dans deux modes : Préférence FIPS et FIPS uniquement. Vous pouvez passer en mode FIPS uniquement après la mise à niveau de tous les composants de votre infrastructure ou lorsqu'ils fonctionnent tous en mode Préférence FIPS.- Vous pouvez revenir au mode Préférence FIPS, si nécessaire.

Informations complémentaires :

Prise en charge de la norme FIPS 140-2 (page 86)

Avant de passer à un autre mode FIPS

Avant de changer le mode FIPS de votre infrastructure Client Automation, vous devez prendre en compte les conditions de fonctionnement dans les différents modes FIPS. Cette section répertorie les remarques et les conditions préalables qui s'appliquent avant de modifier le mode FIPS.

Utilisation de plusieurs modes FIPS

Les restrictions suivantes s'appliquent aux infrastructures Client Automation qui fonctionnent dans plusieurs modes FIPS, avec certains composants en mode Préférence FIPS et d'autres en mode FIPS uniquement :

- Certaines fonctionnalités OSIM peuvent ne pas fonctionner correctement lorsque les composants suivants communiquent entre eux :
  - Gestionnaire de domaines en mode Préférence FIPS et serveur de modularité en mode FIPS uniquement
  - Gestionnaire d'entreprise en mode Préférence FIPS et gestionnaire de domaines en mode FIPS uniquement
- Echec de la communication entre les composants suivants :
  - Composants Client Automation r12 et composants DSM en mode FIPS uniquement

Les remarques suivantes concernent la liaison d'un gestionnaire de domaines vers un gestionnaire d'entreprise :

- Vous pouvez relier uniquement des gestionnaires de domaines utilisant le mode FIPS uniquement à un gestionnaire d'entreprise utilisant le mode FIPS uniquement.
- Vous ne pouvez pas effectuer de liaison si les modes Préférence FIPS (prêt pour le mode FIPS uniquement) ou Préférence FIPS (erreur lors de -l'exécution de dsm_fips_conv) sont définis sur le gestionnaire de domaines ou d'entreprise.
- Si le mode Préférence FIPS est défini sur le gestionnaire d'entreprise, vous pouvez le relier à des gestionnaires de domaines configurés pour les modes Préférence FIPS ou hérités.

Mode Préférence FIPS et mode FIPS uniquement

Les opérations ou fonctionnalités suivantes ne sont pas prises en charge après le passage du mode Préférence FIPS au mode FIPS uniquement :

- Filtres de chiffrement PLAIN et CACRYPT pour le DTS
- Fonctionnalité ADT des transferts fiables et des domaines DTS
- Transfert DTS utilisant la multidiffusion ou la diffusion vers un groupe d'ordinateurs fonctionnant à la fois en mode FIPS uniquement et en mode hérité
- Création et ouverture de fichiers DNA chiffrés à l'aide d'un mot de passe
- Utilisation d'un environnement d'exploitation hérité et d'images de démarrage qui n'ont pas encore été mis à niveau Pour plus d'informations sur la mise à niveau d'images, consultez le *Manuel d'administration du système de gestion des installations de systèmes d'exploitation*.

Configuration requise

Vous devez vérifier que vous avez effectué les opérations suivantes avant de passer à un autre mode FIPS :

- Si vous procédez à la mise à niveau d'un cluster, désactivez le démarrage automatique de Client Automation sur tous les noeuds d'un cluster avant de le mettre à niveau. Vous pouvez activer les services une fois que tous les noeuds du cluster ont été mis à niveau.
- Fermez toutes les instances de l'explorateur DSM (local et distant), de la console Web et des sessions CLI lorsque vous exécutez l'utilitaire de conversion ; ouvrez de nouvelles instances de ces éléments uniquement lorsque l'exécution de l'utilitaire de conversion a pris fin.
- Vérifiez que toutes les stratégies de configuration des gestionnaires d'entreprise et de domaines sont scellées.

Passage en mode FIPS uniquement

Le basculement de l'infrastructure Client Automation vers le mode FIPS uniquement permet l'utilisation de la cryptographie conforme à ce mode. Une fois passés en mode FIPS uniquement, les composants ne peuvent plus communiquer avec les composants r12.

Remarque : Si la cryptographie conforme au mode FIPS uniquement vous semble trop complexe, nous vous recommandons d'utiliser le mode Préférence FIPS.

La procédure suivante décrit les étapes de basculement de l'infrastructure Client Automation en mode FIPS uniquement :

Remarque : Les étapes d'un gestionnaire d'entreprise s'appliquent uniquement si votre environnement inclut un gestionnaire d'entreprise Client Automation.

1. Vérifiez que tous les composants DSM ont été mis à niveau vers Version 12.9.
2. Convertissez toutes les images de système d'exploitation et de démarrage dans un format conforme à la norme FIPS. *Remarque :* Pour plus d'informations sur la mise à jour d'images, reportez-vous au Manuel d'administration du système de gestion des installations de systèmes d'exploitation.
3. Exécutez l'utilitaire de conversion sur le gestionnaire d'entreprise. L'utilitaire convertit les stratégies de configuration globales du système OSIM dans un format conforme à la norme-FIPS, et distribue les valeurs gérées et les définitions de paramètre sur tous les gestionnaires de domaines.
4. Ouvrez le journal d'événements du gestionnaire d'entreprise afin de vérifier que la stratégie a été correctement répliquée vers tous les gestionnaires de domaines.
5. Exécutez l'utilitaire de conversion sur les gestionnaires de domaines. L'utilitaire convertit les stratégies de configuration locales du système OSIM et distribue les valeurs gérées à tous les composants dans l'infrastructure Client Automation.
6. Modifiez la stratégie de configuration par défaut au niveau du gestionnaire d'entreprise pour passer en mode FIPS uniquement.

   Remarque : La modification du mode FIPS via les stratégies de configuration personnalisées n'est pas recommandée.
7. Ouvrez le journal d'événements du gestionnaire d'entreprise afin de vérifier que la stratégie a été correctement répliquée vers tous les gestionnaires de domaines.
8. Si vous ne possédez pas de gestionnaire d'entreprise, modifiez la stratégie de configuration par défaut sur le gestionnaire de domaines pour passer en mode FIPS uniquement.

Remarque : Vous devez redémarrer le cadre d'applications communes pour que le mode FIPS soit activé.

Passage en mode Préférence FIPS

Dans de rares circonstances, vous souhaiterez peut-être que Client Automation communique avec des composants qui ne sont pas conformes à la norme FIPS (un agent hérité par exemple), après avoir basculé l'infrastructure vers le mode FIPS uniquement. Etant donné que le mode FIPS uniquement ne prend pas en charge la rétrocompatibilité, vous devez le faire repasser en mode Préférence-FIPS.

La procédure suivante décrit les étapes de basculement de l'infrastructure en mode Préférence-FIPS :

Remarque : Les étapes d'un gestionnaire d'entreprise s'appliquent uniquement si votre environnement inclut un gestionnaire d'entreprise Client Automation.

1. Modifiez la stratégie de configuration par défaut au niveau du gestionnaire d'entreprise pour passer en mode Préférence FIPS.

   Remarque : La modification du mode FIPS via les stratégies de configuration personnalisées n'est pas recommandée.

2. Ouvrez le journal d'événements du gestionnaire d'entreprise afin de vérifier que la stratégie a été correctement répliquée vers tous les gestionnaires de domaines.

3. Si vous ne possédez pas de gestionnaire d'entreprise, modifiez la stratégie de configuration par défaut sur tous les gestionnaires de domaines pour passer en mode Préférence FIPS.

   Remarque : Vous devez redémarrer le cadre d'applications communes pour que le mode FIPS soit activé. Pour que l'utilitaire de conversion fonctionne, vous devez redémarrer le cadre d'applications communes au moins au niveau du gestionnaire d'entreprise ou de domaines avant d'exécuter l'utilitaire de conversion sur ce gestionnaire.

4. Exécutez l'utilitaire de conversion sur le gestionnaire d'entreprise pour convertir les paramètres globaux du système OSIM à un format rétrocompatible.

5. Ouvrez le journal d'événements du gestionnaire d'entreprise afin de vérifier que la stratégie a été correctement répliquée vers tous les gestionnaires de domaines.

6. Exécutez l'utilitaire de conversion sur le gestionnaire de domaines pour convertir les paramètres locaux du système OSIM à un format rétrocompatible.

Exécution de l'utilitaire de conversion

L'exécution de l'utilitaire de conversion configure les composants DSM afin qu'ils utilisent le mode FIPS requis. Suivez l'ordre suivant pour l'exécution de cet utilitaire :

- Gestionnaire d'entreprise (si présent)
- Gestionnaires de domaines

Pour exécuter l'utilitaire de conversion :

1. Vérifiez que toutes les stratégies de configuration sont scellées au niveau du gestionnaire.
2. Ouvrez la fenêtre de ligne de commande et accédez au dossier *répertoire_installation_ITCM*\bin.
3. Exécutez la commande suivante :

   ```
   dmscript dsm_fips_conv.dms Mode_FIPS
   ```

   Mode_FIPS

   Spécifie le mode FIPS vers lequel vous souhaitez basculer. Les valeurs valides sont FIPS-Only et FIPS-Preferred.

   Une fois les opérations de l'utilitaire terminées, il renvoie un message de réussite ou d'échec. Si vous avez exécuté l'utilitaire avec le paramètre FIPS-ONLY, l'utilitaire change le mode FIPS du gestionnaire correspondant selon que l'exécution de l'utilitaire réussit ou échoue.

4. Ouvrez l'explorateur DSM au niveau du gestionnaire, cliquez sur le noeud racine et recherchez le paramètre FIPS-140 dans le portlet Etat du système.

   Le paramètre FIPS-140 affiche le mode FIPS du gestionnaire.

   - Si l'utilitaire s'est exécuté correctement, ce paramètre affiche Préférence FIPS (prêt pour le mode FIPS uniquement). Vous pouvez, dans ce cas, modifier la stratégie de configuration et changer de mode FIPS.
   - Si l'utilitaire a échoué, le paramètre affiche Préférence-FIPS (erreur lors de l'exécution de dsm_fips_conv)). Le gestionnaire continue à fonctionner dans ce mode jusqu'à la réussite de l'exécution de l'utilitaire de conversion au niveau du gestionnaire.

   Remarque : Les clients r12 (explorateur DSM, CLI, etc.) ne sont pas autorisés à se connecter au gestionnaire, lorsque le gestionnaire fonctionne dans l'un de ces deux modes.

5. Si l'utilitaire s'est terminé avec des erreurs ou des avertissements, procédez comme suit :

   a. Affichez le fichier journal osimfiputil.log dans le dossier *répertoire_installation_ITCM*\bin si le script s'est terminé avec des erreurs ou des avertissements. Pour en savoir plus, consultez le journal d'événements.

   b. Exécutez les actions correctives nécessaires pour corriger les erreurs et relancez l'utilitaire de conversion.

      Les composants DSM sont configurés pour utiliser le mode FIPS requis.

Exemple : commande pour l'exécution de l'utilitaire de conversion pour le mode FIPS uniquement :

```
dmscript dsm_fips_conv.dms FIPS_ONLY
```

Modification de la stratégie de configuration dans le cadre de la modification du mode FIPS

Pour modifier le mode FIPS de votre infrastructure Client Automation, vous devez modifier les stratégies FIPS au niveau de la stratégie de configuration par défaut. Ces stratégies déterminent le mode FIPS vers lequel vous souhaitez basculer ainsi que l'action à exécuter avant de passer d'un mode FIPS à un autre.

Si vous possédez un gestionnaire d'entreprise, effectuez les étapes ci-dessous. Les changements de stratégie sont automatiquement propagés à tous les gestionnaires de domaines associés, aux serveurs de modularité et aux agents. Si vous ne possédez pas de gestionnaire d'entreprise, procédez comme suit sur tous les gestionnaires de domaines.

Remarque : Effectuez cette tâche uniquement si le mode FIPS du gestionnaire est Préférence FIPS (prêt pour le mode FIPS-uniquement).

Pour modifier la stratégie de configuration afin de modifier le mode FIPS :

1. Ouvrez le panneau de configuration et, dans Stratégie de configuration, cliquez avec le bouton droit de la souris sur Stratégie de configuration par défaut, puis cliquez sur Desceller.

   La stratégie est descellée et prête pour les mises à jour.

   Remarque : La modification du mode FIPS via les stratégies de configuration personnalisées n'est pas recommandée.

2. Allez dans DSM, Composants communs, Sécurité, Paramètres FIPS 140 et modifiez les stratégies suivantes :

   Paramètre FIPS 140

   Définit le niveau de conformité à la norme FIPS. Modifiez ce paramètre pour spécifier le mode FIPS vers lequel vous souhaitez basculer.

   Action sur modification

   Définit les actions à exécuter lors de la modification du paramètre FIPS 140.

   Remarque : Pour plus d'informations sur les valeurs de la stratégie pour ces paramètres, consultez l'*aide de l'explorateur DSM*.

3. Scellez la stratégie au niveau du gestionnaire. Pour plus d'informations sur le scellement de la stratégie, consultez la section Stratégie de configuration de l'*aide de l'explorateur DSM*.

   Les changements de stratégie sont propagés à tous les composants DSM associés. Ce processus prend du temps si votre infrastructure Client Automation est volumineuse.

4. Vous devez modifier manuellement le mode FIPS des composants suivants étant donné que les changements de stratégie ne seront pas automatiquement propagés à ces composants :

   - Agents autonomes Remote Control
   - Agents DSM non gérés sur le gestionnaire d'entreprise

     Remarque : Un agent non géré est un agent qui n'est relié à aucun gestionnaire de domaines. Si, par la suite, vous reliez l'agent non géré à un gestionnaire de domaines, le mode FIPS de l'agent sera remplacé par celui du gestionnaire de domaines.

   Pour modifier manuellement le mode FIPS, utilisez la commande suivante :

   ```
   ccnfcmda –cmd setparametervalue –ps /itrm/common/security/fips140 –pn
   installmode –v Mode_FIPS
   ```

   FIPS_MODE

   Spécifie le mode FIPS. Entrez 1 pour activer le mode Préférence FIPS et 2 pour le mode FIPS uniquement.

   Le mode FIPS spécifié est activé au niveau de l'agent, lorsque la commande est exécutée correctement.

   Remarque : L'explorateur DSM autonome et le générateur de rapports DSM ne requièrent aucune configuration spécifique étant donné que l'agent DSM est toujours installé avec l'installation-autonome de ces deux composants et que les agents reçoivent automatiquement la mise à jour de stratégie envoyée par le gestionnaire.

5. Exécutez la commande suivante sur tous les composants DSM si vous n'avez pas modifié le paramètre par défaut de la stratégie Action sur modification ou si vous l'avez défini sur Passer en mode FIPS au prochain redémarrage de CA ITCM :

   ```
   caf stop
   caf start
   ```

   Le gestionnaire fonctionne dans le nouveau mode FIPS une fois le cadre d'applications communes redémarré.

6. Redémarrez toutes les instances de l'explorateur DSM, du générateur de rapports DSM et de la console Web.

   Le mode FIPS actualisé est maintenant disponible dans l'IUG.

7. Vérifiez que le mode FIPS des agents et des gestionnaires a basculé vers le mode FIPS requis.

   La vérification permet d'assurer la réussite du basculement.

   Remarque : Si l'utilitaire de conversion n'est pas exécuté correctement, le mode FIPS du gestionnaire reste Préférence FIPS (erreur lors de l'exécution de dsm_fips_conv).

Affichage du mode FIPS des composants DSM

Vous pouvez afficher le mode FIPS des gestionnaires DSM, des serveurs de modularité et des agents afin de vérifier si l'opération de basculement a réussi. Le mode FIPS est disponible sous forme de données d'inventaire.

Pour afficher le mode FIPS des composants DSM :

1. Dans l'explorateur DSM, cliquez sur le noeud racine.

   Le portlet Etat du système affiche le mode FIPS du gestionnaire.

2. Accédez à Ordinateurs et utilisateurs, Tous les ordinateurs, *nom_ordinateur*, Inventaire, Etat du système.

   L'attribut Mode FIPS dans le volet droit affiche le mode FIPS de l'ordinateur sélectionné.

Remarque : Vous pouvez également exécuter des requêtes et des rapports spécifiques de FIPS pour afficher le mode FIPS de plusieurs ordinateurs agent et du gestionnaire.

Informations complémentaires :

Requêtes et rapports prédéfinis du mode FIPS (page 461)

Requêtes et rapports prédéfinis du mode FIPS

Les requêtes et rapports prédéfinis ci-dessous permettent d'afficher le mode FIPS des composants DSM dans votre infrastructure :

Requêtes

Actifs fonctionnant en mode FIPS uniquement

Actifs fonctionnant en mode Préférence FIPS

Actifs fonctionnant sans prise en charge de la norme FIPS

Rapports

Tous les ordinateurs par mode FIPS

Remarque : Le mode FIPS des ordinateurs d'agent r11.x ou r12 connectés à un gestionnaire de la version Version 12.9 (fonctionnant en mode Préférence FIPS) est défini sur "AUCUN". Le mode FIPS des agents NRI est défini sur "N/D."

Configuration de la conformité à la norme FIPS pour les composants Web DSM

Vous devez configurer votre console Web, votre navigateur et le serveur Web afin de garantir la conformité à la norme FIPS lors de la communication entre les composants Web et les autres composants DSM.

Pour configurer la conformité à la norme FIPS de la console Web Client Automation :

1. Configurez le protocole SSL entre les composants suivants :

    a. Navigateur client et console Web Client Automation

    b. Console Web Client Automation et services Web Client Automation

    Remarque : Pour plus d'informations sur la configuration du protocole TLS 1.0 avec IIS, consultez le livre vert *Securing the Web Admin Console Communication Using SSL* (sécurisation de la communication avec la console d'administration Web à l'aide du protocole SSL). Pour plus d'informations sur la configuration de TLS 1.0 sur le serveur Web Apache, consultez la documentation du serveur Web Apache.

2. Configurez votre navigateur pour qu'il utilise TLS 1.0 pour la communication. Pour plus d'informations, reportez-vous à la documentation du navigateur.

3. Configurez SSL pour qu'il soit conforme à la norme FIPS sur votre serveur Web. Pour plus d'informations, reportez-vous à la documentation de votre serveur Web.

4. Apportez les modifications suivantes au niveau des paramètres du fichier *chemin_installation*\Web Console\webapps\wac\WEB-INF\classes\com\ca\wac\config\WACConfig.properties :

    ```
    AMS_URL=https://nomhôte/AMS/login.do
    WEBSERVICE_URL=https://nomhôte/UDSM_R11_WebService/mod_gsoap.dll (pour
    Windows)
    WEBSERVICE_URL=https://nomhôte/UDSM_R11_WebService (pour Linux)
    SSL_Enabled=True
    TrustStoreFileFullPath=cheminmagasinapprobations
    TrustStorePassword=motdepasse
    ```

    La console Web est configurée pour utiliser TLS pour l'intégralité de la communication.

5. Redémarrez tomcat à l'aide des commandes suivantes :

    ```
    caf stop tomcat
    caf start tomcat
    ```

    Les configurations actualisées prennent effet après le redémarrage de Tomcat.

Réparation d'un agent FIPS uniquement connecté à un composant r12

La communication est impossible entre un agent FIPS uniquement et un gestionnaire ou un serveur de modularité r12, car ils utilisent des modes FIPS incompatibles. Vous devez mettre à niveau le gestionnaire ou le serveur de modularité, ou basculer le mode FIPS de l'agent sur Préférence-FIPS.

Pour modifier le mode FIPS de l'agent sur Préférence-FIPS :

1. Exécutez la commande suivante au niveau de l'agent :

   ```
   ccnfcmda –cmd setparametervalue –ps /itrm/common/security/fips140 –pn
   installmode –v 1
   ```

   Le mode FIPS bascule sur Préférence FIPS au niveau de l'agent lors de l'exécution sans heurt de la commande.

2. Exécutez les commandes suivantes pour redémarrer le cadre d'applications communes :

   ```
   caf stop
   caf start
   ```

   L'agent fonctionne en mode Préférence FIPS, une fois le cadre d'applications communes redémarré.

Scénarios de non-application des modifications de la stratégie FIPS

Lorsque vous modifiez la configuration de la norme FIPS 140 dans la stratégie de configuration et que vous appliquez la stratégie au niveau du gestionnaire, Client Automation utilise la valeur définie dans la stratégie de l'action de modification pour exécuter cette action. Dans les scénarios suivants, les modifications apportées à la stratégie de la norme FIPS ne prennent pas effet et aucune action n'est exécutée sur la base de la stratégie de l'action de modification.

- La stratégie n'a pas encore atteint l'ordinateur cible : vérifiez les paramètres de l'ordinateur cible à l'aide de la commande suivante :

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn policy
  ```

  La commande renvoie 0 (hérité), 1 (Préférence FIPS) ou 2 (FIPS uniquement). Si la commande renvoie la valeur du nouveau mode FIPS, le nouveau mode entrera en vigueur au redémarrage de Client Automation et lors de la copie de la nouvelle valeur dans le paramètre installmode. Si la commande ne renvoie pas la valeur du nouveau mode FIPS, cela indique que la stratégie n'a pas encore atteint l'ordinateur cible.

  Pour obtenir le mode FIPS actuel de l'ordinateur cible, utilisez la commande suivante :

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  installmode
  ```

  Habituellement, le paramètre installmode et le paramètre de la stratégie doivent contenir la même valeur. Toutefois, le paramètre installmode utilisera la valeur de la nouvelle stratégie uniquement sur redémarrage de Client Automation après l'application de la nouvelle stratégie.

  Remarque : Pour plus d'informations sur la commande ccnfcmda de l'agent de configuration, saisissez <command> / ? dans l'invite de commande.

- La stratégie FIPS uniquement est appliquée sur un gestionnaire DSM qui n'a pas exécuté l'utilitaire de conversion ou pour lequel l'utilitaire de conversion ne s'est pas fermé avec des erreurs. Etant donné que le mode FIPS uniquement requiert l'exécution sans heurt de l'utilitaire de conversion, la modification de la stratégie prend effet uniquement lorsque l'utilitaire de conversion est exécuté correctement au niveau du gestionnaire :

  Pour savoir si l'utilitaire de conversion a été exécuté correctement au niveau du gestionnaire, utilisez la commande suivante :

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  ready_for_fips_only
  ```

  Si la commande renvoie le chiffre 1, cela indique que l'utilitaire a été exécuté correctement au niveau du gestionnaire.

  Remarque : L'utilitaire de conversion doit avoir été exécuté correctement si vous essayez de passer du mode Préférence FIPS au mode FIPS uniquement ou inversement.--

- Le nouveau mode FIPS correspond au mode FIPS actuel. Si l'ordinateur cible utilise déjà le nouveau mode FIPS, les modifications ne prennent pas effet sur l'ordinateur cible.
- Si la stratégie d'action de modification est définie sur Demander à l'utilisateur de redémarrer CA ITCM, une boîte de dialogue s'affiche et invite l'utilisateur à indiquer s'il souhaite redémarrer Client Automation lorsque la stratégie atteint l'ordinateur cible. Si cette boîte de dialogue ne s'affiche pas, vérifiez le paramètre restartaction sur l'ordinateur cible à l'aide de la commande suivante :

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  restartaction
  ```

  Si la commande ne renvoie pas le chiffre 2, cela indique que la stratégie n'a pas encore atteint l'ordinateur cible.

  Important : N'activez *pas* l'option "Demander à l'utilisateur de redémarrer CA ITCM" si vous utilisez un serveur terminal, car l'invite est envoyée à tous les utilisateurs de Client Automation sur ce genre de serveur.

Chapitre 12: Connectivité du réseau étendu (ENC)

Ce chapitre traite des sujets suivants :

Introduction à la connectivité du réseau étendu

CA Client Automation (Client Automation) offre la fonctionnalité Connectivité au réseau étendu (ENC) qui permet aux composants et services DSM d'établir des connexions entre les points d'arrivée situés

- derrière des pare-feu personnels ou de réseau
- sur différentes adresses IP

L'ENC fournit un environnement réseau virtuel dans lequel vous pouvez créer des connexions entre différents composants DSM fonctionnant tous derrière différents pare-feux ou DMZ (zones démilitarisées). Cela inclut les gestionnaires d'entreprise, gestionnaires de domaine, IUG, serveurs de modularité et agents.

Important : ENC peut uniquement être utilisée par les applications authentifiées et autorisées à se connecter à des points d'arrivée spécifiques disposant déjà d'applications avec ENC activée installée à des fins très spécifiques. ENC ne fournit pas un canal général à travers le pare-feu pouvant être utilisé par d'autres applications.

Si deux ordinateurs veulent se connecter mais ne peuvent normalement pas le faire en raison de la présence d'un pare-feu, ENC fait en sorte que les deux ordinateurs soient connectés à un troisième ordinateur (Routeur ENC) qui relaie les données entre les deux ordinateurs.

La passerelle ENC fournit des connexions sécurisées via des pare-feu en imposant les éléments suivants :

- Toutes les connexions utilisant le réseau virtuel de la passerelle ENC doivent être correctement authentifiées au moyen de certificats.
- Toutes les connexions doivent disposer des autorisations adéquates. Les règles d'autorisation sont définies par les stratégies et déterminent qui peut se connecter, à quel moment et dans quel but. Ce point est particulièrement important en cas de connexion via un réseau public ou Internet.
- Toutes les tentatives de connexion et autres opérations peuvent être auditées à des fins de sécurité et de dépannage.

Composants ENC

ENC utilise des composants spécifiques dans l'environnement CA Client Automation, dont les éléments suivants :

Client ENC

Est exécuté sur tous les ordinateurs sur lesquelles la passerelle ENC est activée et coordonne toutes les connexions établies par les applications sur le réseau de la passerelle ENC. Les clients ENC maintiennent une connexion vers un serveur de passerelle ENC.

Serveur de passerelle ENC

Se comporte comme un serveur de modularité pour la passerelle ENC en acceptant les connexions et enregistrements des clients ENC et en les transférant au gestionnaire de passerelle ENC. Plusieurs serveurs peuvent être utilisés dans un réseau ENC.

Gestionnaire de passerelle ENC

Organise toutes les connexions entre les points d'arrivée. Le gestionnaire de passerelle ENC connaît tous les serveurs, clients et routeurs de passerelle ENC du fait que ces composants s'enregistrent à leur démarrage. Un seul gestionnaire de passerelle ENC est autorisé dans un réseau ENC.

Routeur de passerelle ENC

Relaie les données entre les points d'arrivée. Plusieurs routeurs peuvent être utilisés dans un réseau ENC.

Adaptateur de socket sécurisé

Etablit le lien entre les applications et le réseau ENC. Il intercepte les appels réseau de faible niveau et les redirige si possible vers les connexions directes, sinon vers les connexions ENC.

Remarque : La passerelle ENC est un programme unique pouvant fonctionner comme gestionnaire, serveur, routeur ou toute combinaison des trois rôles. De même, le gestionnaire possède toujours un serveur. Le rôle est contrôlé par les paramètres suivants dans le magasin de configuration (comstore) : itrm/common/enc/server - MRS, SRS et Router. Si un paramètre possède la valeur de 1, le serveur prend ce rôle.

Plates-formes prises en charge

Les plates-formes de système d'exploitation prises en charge par ENC sont répertoriées dans le chapitre "Environnements d'exploitation pris en charge" des *notes de parution CA Client Automation,* dans la documentation en ligne de Client Automation (Bibliothèque).

Processus de connexion à la passerelle ENC

La fonction Passerelle ENC permet à Client Automation de communiquer avec d'autres ordinateurs derrière des pare-feux. Si deux ordinateurs veulent se connecter mais ne peuvent normalement pas le faire en raison de la présence d'un pare-feu, la passerelle ENC fait en sorte qu'ils se connectent à un troisième ordinateur capable de relayer les données entre les deux ordinateurs.

Dans un réseau de passerelle ENC, le processus de connexion entre deux points d'arrivée (ordinateurs) est le suivant :

- Le point d'arrivée 1 souhaite écouter les connexions sur le même port. Deux ports sont ouverts, l'un réel et l'autre virtuel. Le port réel accepte les connexions directes ; le port virtuel est maintenu par le client ENC et écoute les connexions à la passerelle ENC.
- Le point d'arrivée 2 souhaite se connecter. L'adaptateur de socket tente d'établir une connexion directe. S'il y parvient (cela peut être dans le même réseau), la passerelle ENC n'a plus de rôle à jouer.
- S'il échoue, l'Adaptateur de socket demande au gestionnaire de passerelle ENC d'organiser la connexion.
- Le gestionnaire de passerelle ENC envoie une liste de routeurs de passerelle ENC connus aux deux points d'arrivée. Chaque point d'arrivée envoie une requête ping aux routeurs et renvoie les résultats. Le gestionnaire de passerelle ENC choisit un routeur que les deux points d'arrivée peuvent atteindre et indique à chacun de s'y connecter.
- Chaque point d'arrivée se connecte au routeur de passerelle ENC qui relaie ensuite les données entre les deux points d'arrivée.

Ce processus s'appuie sur des points d'arrivée capables de se connecter de manière sortante à travers des pare-feux situés autour de leurs réseaux, vers des serveurs et des routeurs de passerelle ENC. Aucune connexion entrante n'est jamais établie, donc aucun port entrant n'a besoin d'être ouvert.

Sécurité de la passerelle ENC

La passerelle ENC permet des communications sécurisées à travers des pare-feux grâce aux mécanismes de sécurité suivants :

- Authentification

  Tous les noeuds de la passerelle ENC (clients, gestionnaires, serveurs et routeurs) doivent s'authentifier mutuellement, à l'aide de la sécurité de la couche de transport (TLS) qui n'est autre qu'une version mise à jour de SSL. Cette méthode d'authentification requiert l'installation de certificats à l'aide de Microsoft PKI ou autre élément similaire.

- Autorisation

  Toutes les passerelles ENC sont configurées à l'aide d'un ensemble de règles qui définissent qui est autorisé à faire quoi, à quel moment et à qui. Cela se présente sous la forme suivante :

  - Appartenance au domaine de noeuds (analogues aux groupes NT mais fonctionnant sur d'autres réseaux)
  - Liste blanche des adresses IP Cette liste regroupe les adresses IP autorisées à établir des connexions à la passerelle ENC.
  - Autorisez ou refusez des règles pour chaque opération de la passerelle ENC, telles que la connexion, l'enregistrement, etc., en fonction de l'appartenance au domaine, du moment de la journée, etc.
  - Périodes

Lors de sa première installation, la passerelle ENC est verrouillée. Elle ne possède aucune règle d'autorisation et refuse ainsi toutes les connexions. Ce procédé est approprié du fait que ces serveurs sont généralement tournés vers Internet. Cela peut engendrer des problèmes car Client Automation est utilisé pour maintenir les règles d'autorisation, et un gestionnaire de domaine peut être déconnecté de l'ordinateur qui exécute la passerelle ENC par un pare-feu. Les étapes qui s'y rapportent sont décrites dans la section Scénarios de déploiement.

Authentification

Les deux extrémités d'une connexion sécurisée valident (authentifient) le certificat de leurs homologues (authentification mutuelle), y compris l'autorité émettrice du certificat.

Pour cela, les deux parties doivent avoir confiance en l'autorité tierce émettrice du certificat. L'ENC utilise le fournisseur Microsoft SCHANNEL TLS complété par la bibliothèque WinTrust afin de garantir la confiance du certificat. La confiance des certificats de la racine et (éventuellement) des certificats intermédiaires est fournie par le système d'exploitation à l'aide du magasin de certificats et des API.

Règles d'autorisation de la passerelle ENC

L'infrastructure virtuelle ENC est protégée par authentification, autorisation et audit. L'authentification est réalisée par le protocole TLS de base du secteur et est décrite dans les sections Authentification (page 407) et Authentification de la passerelle ENC. (page 471) Le composant d'audit est également décrit en détails dans la section Evénements d'audit. (page 489)

Cette section décrit de quel manière et à quel endroit l'autorisation est utilisée et se termine par un exemple appliqué.

Termes généraux

La liste suivante présente les termes utilisés dans le contexte des règles d'autorisation. Certains d'entre eux relèvent de la norme industrielle, tandis que d'autres ont été adaptés pour une utilisation par ENC.

Entité de sécurité

Une entité de sécurité est un objet authentifié, toujours sur un ordinateur situé dans ENC, ayant prouvé son identité auprès des serveurs de passerelle. L'objet est toujours référencé par son URI (Uniform Resource Identifier). Cet objet est l'entité qui émet une requête pour accéder à un objet ou une opération sécurisé. Dans ENC, une entité de sécurité est généralement un ordinateur individuel, un ordinateur pouvant être référencé via un domaine (groupe) ou un sous-groupe d'ordinateurs définis par la correspondance par caractère générique avec l'URI.

Objet sécurisé

L'objet sécurisé est la cible d'une requête ou opération d'accès. L'objet sécurisé est toujours un ordinateur nommé d'après son URI, mais des règles d'accès peuvent s'appliquer à un ordinateur unique, un groupe d'ordinateurs correspondant à un caractère générique ou un domaine complet.

Domaine

Un domaine est un regroupement logique d'ordinateurs utilisé par le composant d'autorisation parmi un groupe d'ordinateurs. Dans un scénario de sous-traitant, un domaine représente généralement les ordinateurs au niveau d'une organisation ou d'une unité organisationnelle. Les entités de sécurité sont mappées dans un domaine par le biais d'une correspondance exacte de l'URI ou des correspondances par caractère générique avec l'URI.

Correspondance par caractère générique

ENC peut utiliser la correspondance par caractère générique afin de déterminer l'appartenance au domaine. La correspondance par caractère générique utilise des expressions régulières pour exécuter l'algorithme correspondant.

ENC utilise des expressions régulières compatibles avec le langage de programmation PERL (PCRE, voir http://www.pcre.org/) pour la fonctionnalité de correspondance par caractère générique. Pour connaître la syntaxe complète des expressions PCRE, accédez au site http://perldoc.perl.org/perlre.html.

TACE – Entrée de contrôle d'accès programmé

Une TACE est une règle qui définit si une opération donnée (ou plusieurs opérations) peut être exécutée ou non par une entité de sécurité sur un objet sécurisé à un moment donné. Certaines règles refusent l'accès tandis que d'autre l'autorisent. Les TACE de refus sont prioritaires par rapport à celles d'autorisation. Toute opération ne disposant pas de règles de correspondance est implicitement refusée.

Important : L'heure active d'une entrée de contrôle d'accès est toujours l'heure locale de la cible d'une opération. Si un agent souhaite se connecter à un autre agent dans un autre fuseau horaire, le noeud du gestionnaire de passerelle ENC validera la plage horaire dans le contexte de l'agent cible.

TACL – Liste de contrôle d'accès programmé

Une TACL est une liste de règles TACE.

Noeuds de l'infrastructure

Ce terme désigne les noeuds ENC qui fournissent l'infrastructure de réseau virtuel ENC, dont ceux du gestionnaire, du serveur et du routeur, mais pas les agents ENC eux-mêmes.

URI - Identificateur URI

Un URI est une chaîne utilisée pour nommer ou identifier une ressource. ENC utilise un URI pour représenter tous les objets authentifiés.

ENC et les URI (Uniform Resource Identifiers)

L'autorisation ENC utilise les URI (Uniform Resource Identifiers) pour sa base de données interne. Un URI ENC présente le format suivant :

```
x509cert://[TLS-SCHANNEL]/CN=forward,OU=computers,DC=forward,DC=com
```

x509cert

Indique l'espace de noms. X509cert signifie que l'URI représente une identité de certificat x.509.

[TLS-SCHANNEL]

Indique l'autorité incorporée dans l'URI. Ce nom d'autorité particulier indique que l'authentification est déléguée au fournisseur de sécurité TLS SCHANNEL et au fournisseur WinTrust. Ces fournisseurs gèrent la confiance du certificat pour le compte d'ENC.

CN=forward,OU=computers,DC=forward,DC=dom

Définit le nom d'objet x.500 intégré au certificat. Le format et le contenu réels de ce nom dépendent du fournisseur. L'exemple ci-dessus provient d'un certificat créé par les services de certificats intégrés à Microsoft Active Directory. D'autres infrastructures PKI et la création manuelle de certificats peuvent utiliser d'autres conventions de dénomination.

Pour déterminer l'URI d'un ordinateur par programmation, vous pouvez utiliser l'utilitaire encUtilCmd. L'exécution de la commande "encUtilCmd certv" permet d'afficher les identités de certificats que l'ordinateur utilise pour l'authentification ENC—à la fois comme client et comme serveur, le cas échéant.

Exemple : Commande encutilcmd certv

```
C:\>encutilcmd certv
INFO: L'utilisateur actuel du processus est membre du groupe local
d'administrateurs.
INFO: Le contexte TLS côté client qui a été créé et validé est correct.
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,O=enc
INFO: Le contexte TLS côté serveur qui a été créé et validé est correct.
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,O=enc
```

Configuration des règles d'autorisation

Les règles d'autorisation du service de passerelle ENC sont configurées à partir de l'éditeur de stratégies de configuration DSM. Contrairement aux autres sections de stratégies, il n'existe aucun accès direct aux tables d'autorisation sous-jacentes et la configuration s'effectue par le biais d'une boîte de dialogue personnalisée. La boîte de dialogue gère les dépendances entre les tables et offre une pré-évaluation des règles spécifiées.

La vue de configuration est composée de cinq vues à onglets dans la boîte de dialogue de configuration. Les onglets et leur contenu sont les suivants :

Domaines

Cette vue permet d'afficher ou de définir un domaine ENC et d'ajouter quelques remarques brèves sur le domaine.

Mappage du nom.

Cette vue permet de revoir ou de définir le mappage entre les objets authentifiés et leur appartenance au domaine. Le champ principal est l'identité authentifiée sous forme d'URI. L'URI destiné au mappage du domaine peut se présenter sous la forme d'un URI entièrement spécifié devant correspondre exactement ou d'un URI spécifié en tant qu'expression régulière pour correspondre à plusieurs URI.

Périodes

Tous les contrôles d'accès d'autorisation de l'ENC peuvent être limités dans le temps. Cet onglet permet de définir une période d'utilisation par les entrées de contrôle d'accès individuelles. Les entrées peuvent être des "jours normaux de la semaine", la période s'appliquant à un ou plusieurs jours de dimanche à samedi, ou des "dates spéciales", telles que l'anniversaire de l'indépendance américaine, etc.

Les heures pour lesquelles la période est valide sont indiquées sous forme de période de début et de fin en format 24 heures, par exemple "00:00 - 00:00" pour une période de 24 heures. Le niveau de détail de la période est de 30 minutes. Chaque entrée doit donc utiliser 00 ou 30 comme valeur pour les minutes.

Contrôle d'accès

Cet onglet permet d'accéder aux entrées de contrôle d'accès programmé. Chaque entrée vous permet d'indiquer des règles nommées qui autorisent ou refusent l'activité (les règles conçues pour refuser l'accès ont priorité sur les règles qui l'autorisent). Le nom de la TACE est enregistré dans les entrées d'audit et affiché par la commande de l'utilitaire lors de la simulation d'accès aux règles testées. Par conséquent, il est recommandé d'utiliser des noms descriptifs raisonnables et adaptés à chaque règle.

L'entrée de contrôle d'accès peut contrôler un événement uniquement ou être regroupée pour contrôler plusieurs événements au sein d'une seule règle. Pour chaque règle, nous avons une ressource protégée, l'objet sécurisé, et un objet d'accès, l'entité de sécurité.

Adresses IP

Cet onglet affiche la table de la liste blanche d'adresses IP. Chaque entrée peut être une adresse IP unique ou une plage d'adresses IP spécifiée par une expression de correspondance par caractère générique. Les ordinateurs de l'infrastructure accepteront uniquement les connexions provenant des ordinateurs portant les adresses spécifiées.

Evénements

L'infrastructure ENC définit une série d'événements qui correspondent aux opérations qui requièrent une vérification d'autorisation. La plupart de ces événements peuvent être définis dans une TACE afin de contrôler quelles entités de sécurité sont autorisées à effectuer quelles actions, à qui et à quel moment. Dans la plupart des cas, si le composant d'autorisation refuse la requête d'accès, la connexion physique est interrompue. Les événements de recherche de nom et de connexion d'agent sont des exceptions à cette règle.

Voici une brève description de chacun des événements. Pour chaque événement, l'entrée "objet sécurisé" définit la ressource protégée et l'entrée "entité de sécurité" définit la ressource demandée.

Connexion réseau

Objet sécurisé : Le noeud ENC recevant la connexion.

Cet événement est le seul à ne pas être contrôlé dans la règle TACE ; la cible de l'opération est alors implicite. L'ensemble des accès est contrôlé par la liste blanche d'adresses IP. Seuls les noeud ou plages IP répertoriés dans la liste blanche d'adresses IP sont autorisés à se connecter aux noeuds de l'infrastructure ENC. L'objet sécurisé dans cette instance est toujours le noeud ENC cible. La liste blanche s'applique actuellement à tous les noeuds de l'infrastructure ENC.

Connexion authentifiée

Objet sécurisé : Le noeud ENC acceptant la connexion.

Entité de sécurité : L'identité authentifiée du noeud ENC connecté.

Tous les noeuds doivent s'authentifier une fois qu'ils ont établi une connexion réseau vers un noeud ENC partenaire. Cet événement est généré une fois la séquence d'authentification terminée avec succès. Le noeud ENC acceptant appelle l'API d'autorisation avec l'URI authentifiée du noeud se connectant afin de voir si l'opération est autorisée.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Enregistrement du serveur

Objet sécurisé : Le noeud du gestionnaire de passerelle ENC.

Entité de sécurité : L'identité authentifiée du noeud du serveur de passerelle ENC.

Lorsqu'un serveur de passerelle ENC parvient à établir une connexion authentifiée avec son gestionnaire, il envoie un message d'enregistrement demandant à s'enregistrer en tant que serveur. Le gestionnaire de passerelle ENC appelle ensuite le composant d'autorisation pour déterminer si le serveur est autorisé à s'enregistrer avec ce gestionnaire. Cela permet d'empêcher les serveurs de passerelle ENC non autorisés de se placer dans le réseau virtuel ENC.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Enregistrement du routeur

Objet sécurisé Le serveur de passerelle ENC gérant la requête.

Entité de sécurité : L'identité authentifiée du noeud du routeur de passerelle ENC.

Lorsqu'un routeur parvient à établir une connexion authentifiée avec son serveur, il envoie également un message d'enregistrement demandant à pouvoir s'enregistrer en tant que routeur. Le serveur de passerelle ENC effectue une vérification d'autorisation locale afin de déterminer si cette opération est autorisée, puis transmet la requête au gestionnaire de passerelle ENC pour l'autorisation suivante.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Enregistrement du gestionnaire du routeur

Objet sécurisé : Le noeud du gestionnaire de passerelle ENC.

Entité de sécurité : L'identité authentifiée du noeud du routeur de passerelle ENC.

Cet événement est généré lorsqu'un serveur transfère un message d'enregistrement d'un routeur. Le gestionnaire de passerelle ENC appelle le composant d'autorisation afin de déterminer si le routeur est autorisé à rejoindre le réseau virtuel ENC.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Enregistrement du client su serveur

Objet sécurisé Le serveur de passerelle ENC gérant la requête.

Entité de sécurité : L'identité authentifiée du noeud du client ENC.

Cet événement est généré lorsqu'un noeud de client ENC s'enregistre auprès d'un noeud du serveur de passerelle ENC. Le serveur effectue une vérification d'autorisation locale puis transmet la requête d'enregistrement au gestionnaire de passerelle ENC pour une réponse d'autorisation.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Enregistrement du client du gestionnaire

Objet sécurisé : Le noeud du gestionnaire de passerelle ENC.

Entité de sécurité : L'identité authentifiée du noeud du client ENC.

Cet événement est généré lorsqu'un noeud du serveur de passerelle ENC transfère un message d'enregistrement d'un client ENC au gestionnaire de passerelle ENC.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Ecoute de l'hôte

Cet événement n'est actuellement pas implémenté. L'événement consiste en une vérification d'autorisation locale d'agent visant à déterminer si l'agent ENC est autorisé à créer une connexion d'écoute.

Connexion de l'hôte

Cet événement n'est actuellement pas implémenté. L'événement consiste en une vérification d'autorisation locale d'agent visant à déterminer si l'agent ENC est autorisé à créer une connexion sortante.

Connexion de l'agent

Objet sécurisé : L'identité de sécurité du noeud ENC cible.

Entité de sécurité : L'identité authentifiée du noeud du client ENC demandeur.

Cet événement est généré au niveau du noeud du gestionnaire de passerelle ENC dès qu'un agent ENC souhaite se connecter au noeud d'un autre agent ENC.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Connexion de l'agent au routeur

Objet sécurisé : L'identité de sécurité du noeud ENC du routeur de passerelle ENC.

Entité de sécurité : L'identité authentifiée du noeud du client ENC demandeur.

Cet événement est généré au niveau du noeud du routeur de passerelle ENC lorsqu'un un agent ENC se connecte au routeur afin d'établir une connexion virtuelle vers le noeud d'un autre agent ENC.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs, ou d'un nom de domaine.

Recherche de nom

Objet sécurisé : L'identité de sécurité du noeud ENC cible.

Entité de sécurité : L'identité authentifiée du noeud du client ENC demandeur.

Cet événement est généré au niveau du noeud du gestionnaire de passerelle ENC lorsqu'un noeud ENC souhaite effectuer une opération de recherche de nom pour convertir un nom d'hôte symbolique en adresse privée ENC.

Le gestionnaire de passerelle ENC extrait le nom DNS cible à partir de la requête de recherche de nom puis le convertit en un ou plusieurs enregistrements client (autorisant ainsi les noms d'hôtes dupliqués entre les domaines mais pas à l'intérieur). Ces enregistrements client sont transmis au composant d'autorisation qui décide si la requête de recherche de nom doit être autorisée (ou non). Un enregistrement client consiste en un nom DNS connu et l'identité authentifiée de l'objet.

L'entrée de contrôle d'accès pour cet événement peut spécifier la cible sous forme d'identité littérale de l'ordinateur (à partir de l'authentification), d'un nom de domaine, ou d'une expression de correspondance par caractère générique pour désigner un sous-groupe d'ordinateurs voire plusieurs domaines.

Accès à la gestion

Objet sécurisé : L'identité de sécurité du noeud ENC cible.

Entité de sécurité : L'identité authentifiée du noeud du client ENC demandeur.

Cet événement est généré lorsqu'une connexion du client ENC demande des informations de gestion à partir de la passerelle cible ENC.

Les informations de gestion peuvent inclure des données concernant toutes les connexions virtuelles ENC hébergées par un serveur ENC ; par conséquent, seuls les noeuds approuvés doivent y avoir accès.

Séquence de connexion

Cette section traite la fonctionnalité commune à tous les noeuds ENC et servant à participer à l'infrastructure virtuelle ENC. La fonctionnalité commune est divisée en trois phases distinctes : connexion physique, authentification puis autorisation.

Connexion physique

En premier lieu, tous les noeuds doivent être répertoriés dans la table de la liste blanche d'adresses IP pour être autorisés à se connecter au noeud ENC cible. Sur chaque connexion établie vers un noeud ENC, le composant d'autorisation est appelé à vérifier si l'accès doit être autorisé ou refusé. En cas de refus, la connexion est immédiatement interrompue.

Authentification

Une fois une connexion de transport réseau établie, les homologues impliqués dans la conversation utilisent le protocole TLS pour s'authentifier mutuellement, valident la confiance de l'identité authentifiée, via une autorité de certification tierce approuvée, ainsi que la validité de l'identité.

Autorisation

Suite à la phase d'authentification, l'identité authentifiée est transmise au composant d'autorisation pour la vérification de l'événement "Connexion authentifiée". L'objet sécurisé pour cet événement est le noeud ENC cible. Une règle d'accès visant à autoriser (ou refuser) cette opération peut être spécifiée avec l'ordinateur individuel comme objet sécurisé, un groupe de noms d'ordinateur spécifié à l'aide d'une expression de correspondance par caractère générique ou d'une appartenance au domaine.

Tout échec de la séquence ci-dessus sera audité par le sous-système d'audit de sécurité, si la catégorie ou les messages appropriés sont activés. Le composant d'audit peut également être configuré pour enregistrer toutes les opérations réussies.

Chaque noeud ENC, que ce soit un serveur, un routeur ou un agent client, s'enregistre auprès des noeuds auxquels ils se connectent. Un événement séparé est défini pour chaque type d'enregistrement du fait que seuls les noeuds du serveur de passerelle ENC doivent être autorisés à exécuter une opération d'enregistrement ; seuls les routeurs de passerelle ENC doivent être autorisés à effectuer un enregistrement de routeur, et ainsi de suite.

Selon votre infrastructure, vous pouvez créer des entrées de contrôle d'accès individuelles pour chaque événement et/ou chaque objet sécurisé, ou vous pouvez regrouper les événements et ordinateurs dans un domaine pour un contrôle d'accès moins précis.

Connexions virtuelles ENC

A présent que tous les noeuds de l'infrastructure ENC fonctionnent normalement, nous allons aborder le comportement du réseau virtuel ENC. Dans l'état par défaut, aucune connexion ou recherche de nom n'est autorisée à travers le réseau, sauf s'il existe des entrées de contrôle d'accès explicites visant à les autoriser. Même les ordinateurs regroupés sous un mappage de domaine ne disposent d'aucun droit automatique pour se voir ou se connecter les uns aux autres.

Lorsqu'un noeud d'agent ENC souhaite communiquer avec un autre noeud d'agent ENC, la première opération qui survient consiste généralement en un événement de recherche de noms. Dans la plupart des cas, une seule machine enregistrée portera ce nom donné et elle se trouvera dans le même domaine que la machine envoyant la requête. Elle sera alors couverte par une règle de contrôle d'accès qui autorise tous les noeuds ENC au sein d'un domaine donné à contacter et rechercher d'autres membres de ce domaine. Dans de rares circonstances, il peut exister deux machines, ou plus, portant le même nom complet. Dans cet événement, nous devons désambiguïser la recherche de noms en veillant à pouvoir supprimer uniquement les références des ordinateurs au sein du ou des domaines dont l'objet demandeur est membre. Ce procédé vise à empêcher toute fuite de données à travers les domaines, à moins d'être explicitement autorisée par une règle d'accès.

Si le composant d'autorisation autorise la requête de recherche de noms, l'adresse IP de l'hôte ENC virtuel est renvoyée à l'agent du client ENC. Le client ENC envoie ensuite une requête de connexion d'agent au gestionnaire/serveur de passerelle ENC. Là encore, le gestionnaire de passerelle ENC recherche l'identité sécurisée associée à l'adresse de cette requête et demande une autorisation au système d'autorisation pour l'opération à venir.

Si l'autorisation pour la connexion est accordée, les deux agents, les homologues du circuit de communications virtuel, se connectent aux routeurs de passerelle ENC afin de finaliser la connexion. Cette connexion est à nouveau authentifiée et une autorisation d'accès au routeur est requise.

Exemple de paramétrage de règle

Cet exemple utilise la définition du fichier de l'utilitaire de ligne de commande, à partir de encUtilCmd, pour décrire les règles d'autorisation, procédé analogue à l'explorateur DSM ; les paramètres de règle sont très similaires.

Il est possible de générer un paramètre simple de règles, similaires à celles décrites ci-dessous, à l'aide de l'utilitaire encUtilCmd et sa commande "create". Cela vous permet également de générer un script de test tout en pratiquant les règles.

Les domaines suivants sont utilisés dans cet exemple :

[infrastructure]

Ce domaine est celui utilisé pour contenir tous les noeuds de l'infrastructure (gestionnaires, serveurs, routeurs, etc.). L'infrastructure ENC est gérée par Forward, Inc. Dans cet exemple, le nom de domaine apparaît entre crochets afin de le faire ressortir, mais cela n'est pas une obligation ; tous les noms de domaines sont égaux. Tous les ordinateurs de l'infrastructure possèdent des noms de certificat avec un nom distingué relatif (RDN) de DC=forwardinc,DC=com.

[dsm]

Voici un exemple de domaine regroupant tous les ordinateurs qui constituent l'infrastructure DSM. Nous effectuons une distinction contextuelle entre l'infrastructure ENC et l'infrastructure DSM afin de faciliter la distinction des différents domaines. Tous les ordinateurs DSM possèdent des noms de certificats avec un RDN de DC=forward-dsm,DC=com.

east

Voici un exemple de domaine regroupant tous les ordinateurs de l'entreprise "east". Tous les ordinateurs est possèdent des certificats avec un RDN de DC=east,DC=com.

west

Voici un autre exemple de domaine regroupant tous les ordinateurs de l'entreprise "west". Tous les ordinateurs ouest possèdent des certificats avec un RDN de DC=west,DC=com.

Dans cet exemple, les noeuds ENC, au minimum des noeuds d'agent DSM, sont traités comme des unités autonomes séparées des noeuds DSM. Dans l'environnement ENC DSM, les noeuds du domaine DSM doivent généralement pouvoir voir et se connecter à tous les noms des domaines individuels, et les agents du domaine doivent pouvoir se connecter aux noeuds dans le domaine DSM, mais les membres d'un domaine géré ne peuvent pas voir ni se connecter aux membres d'un autre domaine géré.

Vous devez à présent commencer à définir les règles d'autorisation visant à autoriser l'infrastructure à communiquer et les ordinateurs du domaines à se connecter et à utiliser le réseau virtuel. En premier lieu, vous devez déclarer les domaines pour les autoriser à être utilisés comme références croisées.

Voici un extrait du fichier des règles d'autorisation : la section domaine Elle définit les quatre domaines cités ci-dessus.

```
domaine
{Nom "[infrastructure]" Remarques "Domaine de l'infrastructure ENC"}
{Nom "[dsm]" Remarques "Domaine de l'infrastructure DSM"}
{Nom "east" Remarques "Contact de East Inc. est admin@east.com"}
{Nom "west" Remarques "Contact West Inc. est admin@west.com"}
end
```

La prochaine étape consiste à définir le mappage entre les URI de certificat et les domaines eux-mêmes. Cet exemple utilise la correspondance par caractère générique pour toutes les entrées.

```
URIMapping
{URI ".*,DC=forwardinc,DC=com" Enabled "1" Type "Pattern" Realm
"[infrastructure]"}
{URI ".*,DC=forward-dsm,DC=com" Enabled "1" Type "Pattern" Realm "[dsm]"}
{URI ".*,DC=east,DC=com" Enabled "1" Type "Pattern" Realm "east"}
{URI ".*,DC=west,DC=com" Enabled "1" Type "Pattern" Realm "west"}
end
```

Vous allez ensuite traiter la liste blanche d'adresses IP. Dans cet exemple, vous autorisez deux sous-réseaux IPv4 publiques à accéder à l'infrastructure ENC.

```
IPAddWhiteList
{IPAddress "130\.119\..+" enabled "1" Type "Pattern"}
{IPAddress "141\.202\..+" enabled "1" Type "Pattern"}
{IPAddress "131\.119\..+" enabled "1" Type "Pattern"}
end
```

Le dernier élément à créer avant de passer aux entrées de contrôle d'accès individuelles est une période active. Pour cet exemple, la période est active pour tous les jours de la semaine et couvre les vingt-quatre heures de chaque jour.

```
TimeRange
{Name "all-days" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays "sunday
- saturday"}
end
```

Vous disposez à présent de tous les éléments de base nécessaires pour traiter les règles d'accès ; vous pouvez vous concentrer sur les entrées de contrôle d'accès elles-mêmes. Dans cet exemple, vous utiliserez principalement les entrées de contrôle d'accès individuelles pour des questions de clarté. Dans les situations réelles, il peut s'avérer plus facile et plus efficace de combiner plusieurs règles en une seule.

Voici une entrée de contrôle d'accès unique donnée à titre d'exemple uniquement. Toutes les règles traitées doivent être définies de la manière suivante, entre les balises TimeACL et end, ou créées dans l'IU de configuration.

Cette règle, appelée AC-[infrastructure]-[infrastructure], définit une entrée qui autorise tous les membres du domaine de l'infrastructure à accéder et à s'authentifier à d'autres membres du domaine de l'infrastructure. Elle fait référence à la période "tous les jours" définie précédemment. Elle sera donc active toute la journée et tous les jours.

```
TimeACL
{Name "AC-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow"
TimeRange "all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType
"realm" SecObj "[infrastructure]" Events "AuthenticatedConnection"}
...
end
```

Vous devez ajouter des règles similaires pour les autres domaines, dans ce cas "[dsm]", "est" et "ouest". Les règles seront identiques à celles citées ci-dessus, mis à part que l'entité de sécurité sera remplacée par celle des autres domaines, comme indiqué ci-dessous.

```
{Name "AC-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj
"[infrastructure]" Events "AuthenticatedConnection"}
{Name "AC-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj
"[infrastructure]" Events "AuthenticatedConnection"}
{Name "AC-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj
"[infrastructure]" Events "AuthenticatedConnection"}
```

Vous allez à présent définir d'autres entrées de l'infrastructure. Ces entrées sont accompagnées de commentaires expliquant leur objectif. Comme indiqué ci-dessus, ces entrées peuvent être regroupées en une seule avec le champ Evénement défini sur "ManagerRegisterServer ServerRegisterRouter ManagerRegisterRouter ManagerRegisterAgent". L'avantage de conserver les règles séparées réside dans le fait que les outils de vérification et la consignation de l'audit dans les sous-systèmes ENC utiliseront le nom de règle unique lorsqu'ils expliqueront pour quelle raison une opération a été autorisée ou refusée.

```
; Cette entrée autorise tous les noeuds de l'infrastructure à enregistrer un
serveur sur un gestionnaire.
{Name "MRS-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow"
TimeRange "all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType
"realm" SecObj "[infrastructure]" Events "ManagerRegisterServer"}
;
; Cette entrée autorise tous les noeuds de l'infrastructure à enregistrer un
routeur sur un serveur.
{Name "SRR-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow"
TimeRange "all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType
"realm" SecObj "[infrastructure]" Events "ServerRegisterRouter"}
;
; Cette entrée autorise tous les noeuds de l'infrastructure à enregistrer un
routeur sur un gestionnaire.
{Name "MRR-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow"
TimeRange "all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType
"realm" SecObj "[infrastructure]" Events "ManagerRegisterRouter"}
;
; Cette entrée autorise tous les noeuds de l'infrastructure à enregistrer un
client sur un gestionnaire.
{Name "MRA-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow"
TimeRange "all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType
"realm" SecObj "[infrastructure]" Events "ManagerRegisterAgent"}
```

Vous devez à présent autoriser les domaines DSM et gérés à s'enregistrer avec les noeuds de l'infrastructure. Les entrées suivantes créent cette configuration.

```
{Name "SRA-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj
"[infrastructure]" Events "ServerRegisterAgent"}
```

```
{Name "SRA-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj
"[infrastructure]" Events "ServerRegisterAgent"}
```

```
{Name "SRA-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj
"[infrastructure]" Events "ServerRegisterAgent"}
```

Les routeurs de passerelle ENC nécessitent également la configuration d'autorisation pour tous les noeuds qui y seront connectés et routés. Les entrées suivantes définissent cette configuration.

```
; Ces entrées autorisent tous les noeuds DSM à se connecter aux routeurs dans le
domaine de l'infrastructure.
{Name "RAC-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj
"[infrastructure]" Events "RouterAgentConnect"}
```

```
; Ces entrées autorisent tous les noeuds d'agent du ou des domaines nommés à se
connecter aux routeurs dans le domaine de l'infrastructure.
{Name "RAC-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj
"[infrastructure]" Events "RouterAgentConnect"}
{Name "RAC-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-
days" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj
"[infrastructure]" Events "RouterAgentConnect"}
```

Vous possédez à présent suffisamment de données de configuration pour autoriser tous les noeuds ENC des domaines DSM et gérés à se connecter, s'authentifier et s'enregistrer auprès de tous les noeuds de l'infrastructure ENC. La prochaine étape consiste à autoriser les fonctions de recherche de noms et de connexion d'agent. Les entrées suivantes définissent cette configuration.

Il existe des règles miroirs pour tous les noeuds : les domaines gérés sont autorisés à rechercher les noms de tous les ordinateurs DSM connectés à ENC. Ceux-ci sont à leur tour autorisés à rechercher tous les membres des domaines gérés. Les règles et règles miroirs doivent être explicitement spécifiées, comme indiqué ci-dessous.

Notez qu'il n'existe aucune règle autorisant "est" à voir "ouest" ; inversement, il n'existe aucune règle autorisant "ouest" à voir "est", ce qui rend toute recherche entre les domaines impossible. Cette séparation d'espace de noms est essentielle pour sécuriser le fonctionnement du réseau virtuel.

```
; Ces entrées autorisent tous les noeuds d'agent des domaines nommés à effectuer
des recherches de membres ENC dans le domaine DSM.
{Name "NL-east-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events
"ManagerNameLookup"}
{Name "NL-west-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events
"ManagerNameLookup"}

; Ces entrées autorisent tous les noeuds DSM à effectuer des recherches des
membres ENC dans les domaines nommés.
{Name "NL-[dsm]-east" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "east" Events
"ManagerNameLookup"}
{Name "NL-[dsm]-west" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "west" Events
"ManagerNameLookup"}
```

Les entrées suivantes autorisent les agents à se connecter vers/à partir des domaines DSM et gérés. A nouveau, ces entrées auraient pu être combinées au paramètre de règle précédent, mais la séparation permet une consignation plus détaillée et le dépannage des règles.

```
; Ces entrées autorisent tous les noeuds d'agent des domaines nommés à se
connecter aux membres ENC dans le domaine DSM.
{Name "ACN-east-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events
"AgentConnect"}
{Name "ACN-west-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events
"AgentConnect"}

; Ces entrées autorisent tous les noeuds DSM à se connecter aux membres ENC dans
les domaines nommés.
{Name "ACN-[dsm]-east" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "east" Events
"AgentConnect"}
{Name "ACN-[dsm]-west" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "west" Events
"AgentConnect"}
```

Ceci conclut l'exemple de paramètre de règle.

Procédure et autres questions

Cette section tente d'anticiper les questions susceptibles de se poser et d'y apporter une réponse concise.

J'utilise l'appartenance spéciale à tous les domaines (*) mais les périodes ne sont pas respectées ; pour quelle raison ?

Le caractère * désigne l'objet ordinateur comme membre de tous les domaines et implique qu'il est un "super-utilisateur". Un objet disposant d'un accès super-utilisateur peut effectuer toutes les opérations. Par conséquent, le sous-système d'autorisation autorise toujours l'opération spécifiée, quelles que soient les restrictions de temps ou d'accès. Un domaine super-utilisateur peut tout faire, se connecter partout, rechercher tout, etc. Sachez que l'utilisation du type super-utilisateur est auditée à l'aide d'un avertissement consigné dans le journal d'application système.

Existe-t-il un moyen de vérifier les règles avant de les appliquer ?

Oui, utilisez la commande de l'utilitaire ENC encUtilCmd et la commande "verify". Cela vous permet de simuler tous les événements répertoriés précédemment. Pour des instructions plus détaillées sur la manière d'utiliser l'application, consultez le manuel de référence UtilCmd.

Je dois créer un très grand nombre de règles ! Existe-t-il une méthode plus simple ?

Oui. A nouveau, utilisez la commande de l'utilitaire ENC encUtilCmd. La commande "create" vous permet de créer un ensemble de règles pour plusieurs domaines et de définir un ensemble de règles de base qui reflète l'approche de cette section du document. Vous pouvez également créer simultanément un script de test qui vérifiera toutes les règles créées à l'aide des identités simulées. Vous pouvez ensuite modifier les règles générées pour utiliser les identités de sécurité réelles et personnaliser les autres zones pour satisfaire vos exigences spécifiques.

Evénements d'audit

La passerelle ENC audite en interne les événements sur les connexions entre les noeuds et génère des informations d'audit dans le journal des événements du système d'exploitation. Celles-ci peuvent également être envoyées vers le système Event Management ou un fichier texte. Les événements d'audit sont regroupés en catégories couvrant les erreurs, les connexions, la sécurité, etc. Les événements peuvent être activés ou désactivés individuellement ou par catégories.

Par défaut, toutes les catégories d'audit sont désactivées, à l'exception de la catégorie Erreurs, bien que tous les messages soient activés dans leurs catégories. Et ce afin d'éviter que le journal des événements ne soit submergé par les événements ENC. L'administrateur doit activer les événements nécessaires en cas de dépannage ou de surveillance du fonctionnement du système.

Les événements d'audit peuvent être activés en activant la catégorie correspondante ou l'ensemble des événements peut être activé en configurant un paramètre unique.

Sachez également que, par défaut, toutes les données de configuration d'audit sont gérées localement mais peuvent facilement être transposées en une gestion centrale à l'aide de l'éditeur de stratégies dans l'explorateur DSM.

Pour connaître la liste complète des catégories d'événements, consultez la rubrique "Passerelle ENC et Groupe de stratégies audit du client" dans la section Stratégie de configuration de *l'aide de l'explorateur DSM.*

Installation et configuration des composants de la passerelle ENC

L'installation de la fonctionnalité Passerelle ENC est prise en charge par le programme d'installation de CA Client Automation, actuellement uniquement pour les environnements d'exploitation Windows.

La configuration des composants de la passerelle ENC s'effectue via les paramètres du magasin de configuration (comstore) et est écartée comme une stratégie de configuration gérée.

La fonction Passerelle ENC est désactivée par défaut, car il est supposé que la majorité des installations CA Client Automation sont effectuées dans les réseaux de l'entreprise et n'ont pas besoin de traverser les pare-feux Internet ou internes.

Remarque : Si vous prévoyez d'exécuter un serveur Web de type IIS ou Apache sur le même ordinateur que le serveur de passerelle ENC, ils doivent être configurés de manière à ne pas tenter d'ouvrir les mêmes ports. Par défaut, ENC écoute sur les ports 80 et 443. IIS et Apache écoutent également sur le port 80. Enfin, IISadmin écoute sur le n° 443. Si un conflit de port survient et qu'ENC est incapable d'écouter, un événement correspondant sera consigné dans le journal des événements du système.

Configuration ENC et SSA

La configuration des composants ENC est faite à l'aide de paramètres de configuration communs et transmise par une stratégie de configuration gérée. Si la stratégie de configuration pour ENC ou SSA est modifiée, cela peut entraîner le redémarrage de SSA PMUX et de CAM. Pour plus d'informations sur les stratégies de configuration ENC, reportez-vous à Groupe de stratégies de la passerelle ENC dans la section Stratégie de configuration de l'*Aide de l'explorateur DSM*.

Comment activer le client ENC

Par défaut, le programme d'installation DSM copie les fichiers pour le client ENC sur le disque mais ne les active pas. Si vous décidez d'activer le client ultérieurement, vous devez suivre un certain nombre d'étapes effectuées dans le programme de l'utilitaire encUtilCmd.

Pour activer le client, exécutez les commandes suivantes :

```
//si requis par l'environnement réseau
encutilcmd client -proxy_http [proxy_socks] -proxy_host nom_complet_serveur_proxy
-proxy_port proxy_port_number
        -user nomutilisateur -password motdepasse

encUtilCmd client -state enabled -server Nom_du_serveur_de_passerelle [-port n]
caf start
```

Remarque : L'activation du client aura pour effet secondaire le redémarrage de CA Message Queuing (CAM) et de Secure Socket Adapter Port Multiplexer (SSA PMUX). Cela est dû au fait que ENC s'intègre à ces deux composants et qu'un redémarrage est requis pour les rendre "conscients d'ENC".

Déploiement dans un environnement ENC

Pour réussir le déploiement d'un logiciel dans un environnement ENC, c'est-à-dire avec un pare-feu au milieu, les conditions préalables suivantes sont requises :

- Le composant Déploiement de l'infrastructure de Client Automation requiert la présence de DMPrimer et du fichier dmkeydat.cer (certificat de déploiement) sur l'ordinateur cible.

  Pour plus de détails sur cette étape, consultez les sections Installation manuelle du logiciel d'injection de déploiement de l'infrastructure (page 257) et Fourniture de la clé de sécurité de gestion du déploiement sur une installation du logiciel d'injection (page 258).

- Le composant Client ENC doit être en cours d'exécution et opérationnel sur l'ordinateur cible. Le composant Client ENC est installé avec le composant Inventaire matériel de base et est rendu opérationnel en paramétrant sa configuration.
- Les options de stratégie "Utiliser des noms d'hôtes" et "Ne pas exécuter la commande ping sur la cible lors d'une analyse" de la fonction Déploiement de l'infrastructure doivent être définies sur True.
- L'option de stratégie Toujours déployer un logiciel d'injection doit être définie sur False. En effet, les cibles disposent souvent d'un pare-feu dans les environnements ENC, ce qui empêche l'utilisation des méthodes habituelles pour le déploiement du logiciel d'injection et oblige à utiliser une autre méthode.

Scénarios de déploiement ENC

Les scénarios décrits dans cette section sont censés être les plus courants pour l'utilisation de la fonctionnalité Passerelle ENC. Ils se basent sur le schéma pilote, la succursale et le sous-traitant informatique.

Dans le scénario sous-traitant, des entreprises de différentes tailles ont sous-traité la gestion de leurs bureaux et serveurs à une entreprise spécialisée dans la gestion informatique. CA Client Automation est utilisé pour effectuer les tâches habituelles de gestion technique, mais requiert la fonctionnalité Passerelle ENC pour travailler au-delà des pare-feux et sur Internet. Une entreprise sous-traitante peut naturellement gérer tous les scénarios simultanément, et à plusieurs reprises.

Bien d'autres scénarios sont évidemment possibles.

Dans chaque scénario, les étapes requises pour l'installation et la configuration du système sont décrites et les résultats attendus.

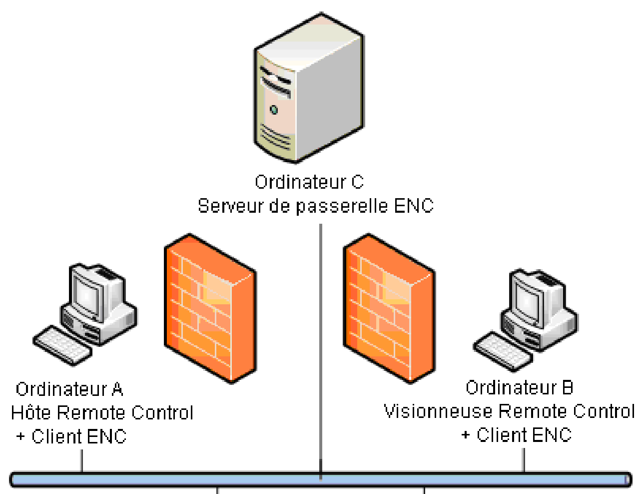
Les scénarios de déploiement ENC considérés dans les sections suivantes sont :

Scénario de déploiement ENC - Le schéma pilote

Ce scénario est censé être le premier qu'une organisation déploie et est destiné à fournir une expérience de la manière dont le système fonctionne. Il sert également d'exemple unique pour faciliter la compréhension de la passerelle ENC.

Ce scénario se base simplement sur trois ordinateurs, les deux premiers étant des ordinateurs d'agent placés derrière des pare-feux personnels Windows et le troisième étant un serveur de passerelle ENC qui fournit la connectivité.

L'illustration suivante présente la configuration du scénario du schéma pilote :



Dans ce scénario, l'ordinateur A exécute un hôte Remote Control, l'ordinateur B exécute une visionneuse Remote Control et l'ordinateur C exécute un serveur de passerelle ENC. L'ordinateur B ne peut pas se connecter à l'ordinateur A car il se trouve derrière un pare-feu. Tous les ordinateurs exécutent des clients ENC connectés au serveur de passerelle ENC sur l'ordinateur C. C'est ce dernier qui fournit la connectivité à partir des ordinateurs B et A. La configuration n'est pas gérée par un gestionnaire de domaine car nous voulons un scénario aussi simple que possible.

Pour configurer un petit réseau de passerelle ENC, suivez les étapes ci-dessous :

Sur l'ordinateur A :

1. Activez le pare-feu Windows.
2. Lancez une installation personnalisée de Client Automation. Sélectionnez "Remote Control" et "Agent".
3. Lorsque le programme d'installation vous demande l'adresse du serveur de modularité, acceptez la valeur par défaut prédéfinie. Lorsque le programme d'installation vous demande de confirmer (du fait qu'il n'y a pas de serveur), cliquez sur Oui. Une installation non gérée peut ainsi fonctionner.
4. Cliquez sur "Client ENC" pour commencer à configurer le client. Entrez l'adresse de l'ordinateur C pour l'adresse du serveur du client.
5. Cliquez sur Remote Control et sélectionnez uniquement "Installer la fonctionnalité Hôte".

6. Une fois l'installation terminée, ne démarrez pas Client Automation, mais exécutez les commandes suivantes :

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn
   centralizedsecurity -v 0
   ```

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn standalone -v 1
   ```

7. Démarrez Client Automation à l'aide de la commande "caf start".

Sur l'ordinateur B :

1. Activez le pare-feu Windows.
2. Lancez une installation personnalisée. Sélectionnez "Remote Control" et "Visionneuse".
3. Aucune spécification de serveur de modularité (procédez comme sur l'ordinateur A).
4. Configurez un client ENC de la même manière que sur l'ordinateur A.
5. Cliquez sur Remote Control et sélectionnez uniquement "Installer la fonctionnalité Visionneuse".
6. Une fois l'installation terminée, ne démarrez pas Client Automation, mais exécutez les commandes suivantes :

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/viewer/managed -pn managedmode -v
   0
   ```

7. Démarrez Client Automation à l'aide de la commande "caf start".

Sur l'ordinateur C :

1. Vérifiez que le pare-feu Windows est désactivé.
2. Lancez une installation personnalisée. Effacez tous les produits. Dans la boîte de dialogue d'installation personnalisée, décochez tous les éléments sauf "Passerelle ENC" et "Agent".
3. Aucune spécification de serveur de modularité (procédez comme sur les ordinateurs A et C).
4. Sur la boîte de dialogue de configuration de la passerelle ENC, sélectionnez les trois rôles : gestionnaire, serveur et routeur.
5. Ne démarrez pas encore Client Automation sur cet ordinateur. La sécurité pour le serveur de passerelle n'est pas encore configurée et rejettera toutes les connexions des clients. Pour configurer la sécurité ENC, nous pouvons créer un fichier texte contenant une règle qui permet à tout le monde de se connecter. Le fichier est ensuite importé dans le magasin commun pour que le serveur y effectue sa sélection.

   Important : Notez que ceci n'est qu'un exemple. Dans un environnement de production réel, vous n'utiliseriez jamais des règles qui autorisent un accès ouvert !

6. Créez un fichier texte appelé defrules.txt et contenant le texte suivant :

```
[authz]
RulesVersion=5

DOMAINE
{Name "ENC" Notes "Le domaine par défaut auquel tout le monde appartient"}
end

TimeRange
{Name "all-days" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays
"sunday - saturday"}
end

TimeACL
{Name "policy1" enabled "1" RuleType "allow" Events "AuthenticatedConnection
ManagerRegisterServer ServerRegisterRouter ManagerRegisterRouter
ServerRegisterAgent ManagerRegisterAgent ManagerNameLookup AgentConnect
RouterAgentConnect ManagementAccess" TimeRange "all-days" SecPrincType
"realm" SecPrinc "ENC" SecObj "ENC" SecObjType "realm"}
end

URIMapping
{URI ".+" enabled "1" Type "pattern" Realm "ENC"}
end

IPAddWhiteList
{IPAddress ".+" enabled "1" Type "pattern"}
end
```

7. Importez ce fichier de règle à l'aide de la commande encUtilCmd, comme suit :

   ```
   encUtilCmd import -i defrules.txt -fl
   ```

   Le serveur de passerelle ENC possède à présent une règle qui autorise toutes les connexions.

8. Enfin, installez les certificats ENC sur tous les ordinateurs. Pour plus d'informations, consultez Configuration des services de certificats pour une utilisation par la passerelle ENC (page 508).

Pour tester le scénario, suivez les étapes ci-après :

1. Sur les ordinateurs A et B, démarrez Client Automation à l'aide de la commande "caf start". Ne démarrez pas encore l'ordinateur C car nous voulons effectuer le test sans la fonctionnalité Passerelle ENC.

2. Démarrez la boîte de dialogue de configuration de l'hôte en la sélectionnant dans la barre d'état système sur l'ordinateur A. Sélectionnez l'onglet Utilisateurs et assurez-vous que l'administrateur local est un utilisateur de Remote Control sur cet ordinateur.

3. Sur l'ordinateur B, démarrez la visionneuse et essayez de vous connecter. Cela doit être bloqué par le pare-feu sur l'ordinateur A.

4. Démarrez Client Automation sur l'ordinateur C. Au bout de quelques minutes, vérifiez que les clients ENC se sont enregistrés auprès du serveur de passerelle ENC à l'aide de la commande encclient status. Cette commande doit indiquer que le client s'est enregistré avec succès et est prêt.

5. Répétez la tentative de connexion ; cela devrait à présent fonctionner. Toutes les données sont acheminées via l'ordinateur C. La commande "encclient status" doit indiquer qu'une connexion est en cours via l'ordinateur C.

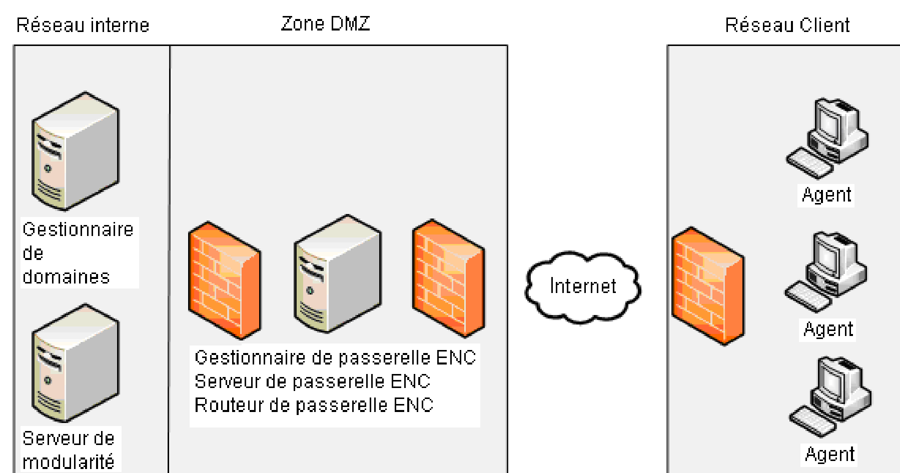
6. Vous pouvez adapter les règles en modifiant le fichier defrules.txt et en le réimportant, mais à l'aide de la commande encUtilCmd avec l'option -o afin de remplacer les règles existantes. Cela vous permet d'expérimenter les différentes règles d'autorisation afin de vous familiariser avec le système.

   Pour une description détaillée de la commande encUtilCmd et de toutes ses options, consultez le document *Référence de la commande encUtilCmd* que vous trouverez dans la *bibliothèque CA*, dans la catégorie Manuels de référence.

Scénario de déploiement ENC - La succursale

Dans ce scénario, l'entreprise parent maintient le gestionnaire de domaine et le serveur de modularité sur le réseau du siège (réseau interne). La succursale possède un LAN avec des agents DSM installés sur leurs ordinateurs (réseau client). Toutes deux sont protégées par des pare-feux et connectées à Internet.

L'illustration suivante présente la configuration réseau dans un exemple de scénario de déploiement de succursale :



Dans ce scénario, nous supposons que tous les ordinateurs du réseau, y compris les ordinateurs du serveur de passerelle ENC, ont au moins un agent DSM installé.

La DMZ (zone démilitarisée) permet la connectivité à partir du réseau interne vers la DMZ, mais pas au-delà. Les ordinateurs de la DMZ peuvent se connecter à Internet mais pas au réseau interne.

Les étapes de déploiement et de configuration requises dans ce scénario sont les suivantes :

- Déploiement de l'infrastructure ENC au siège (réseau interne)
- Déploiement des agents DSM dans la succursale (réseau client)
- Configuration des agents dans la succursale afin de rendre compte au serveur de modularité du siège

Sur le réseau du siège, les activités suivantes s'appliquent :

- Créez une DMZ dans le réseau du siège si celle-ci n'est pas déjà présente. Cette étape est nécessaire car les serveurs de passerelle ENC doivent être visibles par la succursale, qui est supposée se connecter sur l'Internet publique.
- Installez un gestionnaire de domaine DSM, un serveur de modularité, des agents et les clients ENC comme requis dans le réseau parent.
- Installez un agent DSM, un client ENC, gestionnaire, serveur et routeur sur un ordinateur dans la DMZ du réseau du siège. Configurez l'agent pour s'enregistrer auprès du serveur de modularité dans le réseau interne.
- Installez les certificats ENC sur tous les ordinateurs connaissant la passerelle ENC, comme décrit dans la section Gestion des certificats. (page 508) Ceux-ci couvrent les ordinateurs dans le réseau interne et la DMZ. Ils sont requis pour l'authentification de la passerelle ENC.
- Installez les certificats ENC sur les ordinateurs DMZ.
- Ne démarrez pas encore les serveurs de passerelle ENC. A ce stade, le serveur de passerelle ENC est configuré sans aucune règle d'autorisation et rejettera ainsi toutes les connexions. Cela signifie que l'infrastructure DSM dans la DMZ ne peut pas contacter le gestionnaire de domaine dans le réseau du siège et ne peut donc pas recevoir une stratégie de configuration contenant les règles d'autorisation.
- Ouvrez l'explorateur DSM et configurez la stratégie de configuration requise pour ENC. Configurez la passerelle ENC à l'aide d'une stratégie de sécurité. Celle-ci doit couvrir l'accès pour les ordinateurs du réseau du siège ainsi que ceux de la succursale. Toutefois, pour le moment cette stratégie ne peut pas être envoyée aux serveurs de passerelle ENC à partir du gestionnaire de domaine en raison d'un catch-22, c'est-à-dire que l'ordinateur ne peut pas recevoir une stratégie tant qu'il n'est pas enregistré auprès du gestionnaire de domaine, et il ne peut pas s'enregistrer tant qu'il n'obtient pas une stratégie qui définit les règles d'autorisation qui lui permettent de se connecter au gestionnaire de domaine.

- Pour y remédier, le serveur de passerelle ENC doit être "amorcé" à l'aide de règles suffisantes pour autoriser une connexion au gestionnaire de domaine. Une fois celle-ci établie, le gestionnaire de domaine peut envoyer la stratégie réelle afin de remplacer la stratégie d'amorce.

  La stratégie réelle doit auparavant être saisie dans la stratégie de configuration sur le gestionnaire de domaine. Pour ce faire, deux méthodes sont possibles :

  1. La première méthode consiste à ouvrir l'explorateur DSM et à configurer la stratégie de sécurité requise pour ENC à l'aide de l'éditeur de stratégies de configuration. L'IUG propose une boîte de dialogue personnalisée pour vous aider à composer ces règles.
  2. La méthode alternative consiste à composer une fichier texte à l'aide de vos règles par défaut puis de les importer en bloc avec l'utilitaire encUtilCmd. (Pour une description détaillée de la commande encUtilCmd et toutes ses options, consultez le document *Référence de la commande EncUtilCmd*, disponible dans la *bibliothèque CA* dans la catégorie Manuels de référence.) Notez que encUtilCmd représente également un moyen de vérifier les règles avant de les appliquer.

  Ces règles doivent autoriser au minimum l'infrastructure DSM dans le réseau du siège à contacter et s'enregistrer auprès de l'infrastructure de passerelle ENC dans la DMZ.

  Nous vous suggérons de composer les règles en suivant la seconde méthode, car le fichier de règles que vous créez peut ensuite être utilisé sur le gestionnaire de domaine et les ordinateurs du serveur ENC. L'IUG peut être utilisée pour apporter des modifications ultérieures à la stratégie.

  Appliquez les règles au gestionnaire de domaine à l'aide de la commande "encUtilCmd importdb". Celle-ci ajoute les règles à la base de données de configuration DSM. Une fois ajoutées, elles peuvent être transmises via le mécanisme de stratégie habituel lorsque les ordinateurs du serveur ENC se connectent.

  Appliquez ces règles au serveur de passerelle ENC dans la DMZ à l'aide de la commande "encUtilCmd import". Cela amorcera le serveur avec les règles d'autorisation et autorisera l'ordinateur à contacter le gestionnaire de domaine et à s'enregistrer.

  Démarrez CA Client Automation sur les serveurs de passerelle ENC afin qu'ils sélectionnent les nouvelles règles et qu'ils autorisent l'établissement des connexions ENC.

- Par défaut, la stratégie de configuration dans le gestionnaire de domaine est définie pour être gérée localement afin d'éviter tout écrasement accidentel par une stratégie vide. Définissez-la sur une gestion centralisée. Lorsque l'enregistrement de CA Client Automation réussit, la règle par défaut initiale est écrasée par la stratégie envoyée en aval par le gestionnaire de domaine.

- Patientez 10 minutes puis vérifiez que les ordinateurs dans la DMZ se sont enregistrés et sont visibles dans l'IUG.
- Si aucun ordinateur n'est visible, il se peut que les règles par défaut soit erronées ou que la nouvelle stratégie ait interrompu l'accès. Afin d'obtenir un diagnostic, examinez le journal des événements de l'application NT sur les serveurs de passerelle ENC.

Sur le réseau de la succursale, les activités suivantes s'appliquent :

- Installez les agents DSM requis sur chaque ordinateur du réseau de la succursale. La fonctionnalité Passerelle ENC est installée par défaut mais nécessite une configuration spécifique. Configurez les clients afin qu'ils s'enregistrent auprès du serveur de passerelle ENC dans la DMZ du réseau du siège. Du fait que la passerelle ENC ne fonctionne pas encore entre le siège et la succursale, le déploiement DSM ne peut pas être utilisé. L'installation peut alors être exécutée à l'aide d'un certain nombre de méthodes qui dépendent du nombre d'ordinateurs impliqués, par exemple :
  - Installation manuelle à partir du DVD, si seul un petit nombre d'ordinateurs sont installés
  - Installation d'un package à l'ouverture de session de l'utilisateur à partir d'un script de connexion au domaine NT.
  - Installation d'un gestionnaire de domaine et d'un serveur de modularité temporaires au sein du réseau de la succursale. Pour cela, utilisez une machine réelle ou virtuelle envoyée vers la succursale. Utilisez la fonctionnalité de déploiement de CA Client Automation pour envoyer le package de l'agent. Une fois le déploiement terminé et tous les agents enregistrés auprès du gestionnaire de domaine du siège, le gestionnaire de domaine temporaire est supprimée dans la succursale.
- Vérifiez que les ordinateurs de la succursale s'enregistrent en vérifiant que le groupe Tous les ordinateurs est à nouveau dans l'IUG du siège.
- Effectuez les tests de validation habituels utilisés par votre organisation afin de garantir que <udsk> est entièrement fonctionnel.

Scénario de déploiement ENC - Petite entreprise cliente sous-traitante

Le scénario pour petite entreprise est très similaire à celui de la succursale, à l'exception du niveau de sécurité supplémentaire requis. Comme le sous-traitant peut être en charge d'un grande nombre d'entreprises, un contrôle plus strict doit être imposé à la connectivité autorisée entre les noeuds dans chaque réseau de l'entreprise. En outre, l'accès d'un client sous-traité à un autre client doit être sécurisé. Normalement, un client ne serait pas autorisé à voir les ordinateurs d'un autre. Cette situation est gérée par la prise en charge des domaines dans l'autorisation de la passerelle ENC.

Les ordinateurs de l'entreprise sous-traitante doivent pouvoir se connecter aux ordinateurs du client. Cela nécessite la configuration du gestionnaire de passerelle ENC du sous-traitant avec les règles d'autorisation qui permettent les opérations suivantes :

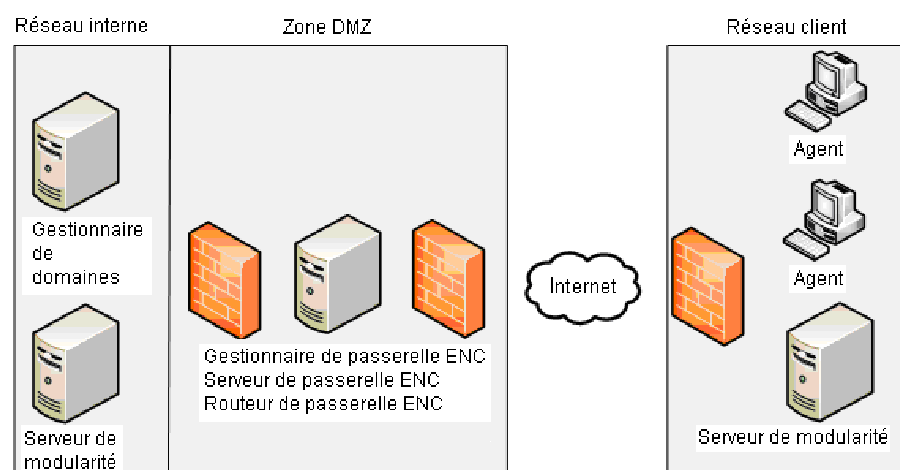
- Enregistrement des ordinateurs dans le réseau client.
- Connexions des ordinateurs du réseau client aux ordinateurs du réseau sous-traitant, et inversement.
- Les connexions entre les différents domaines clients sont refusées.

La configuration de Client Automation est similaire, mais la gestion de la zone de sécurité doit également être configurée pour gérer les exigences de sécurité (voir le chapitre "Fonctionnalités de sécurité Client Automation" (page 407)).

Scénario de déploiement ENC - Moyenne entreprise cliente sous-traitante

Dans ce scénario, le client dispose de suffisamment d'ordinateurs pour garantir son propre serveur de modularité.

L'illustration suivante présente la configuration réseau dans un exemple de scénario de déploiement dans une entreprise cliente sous-traitante moyenne :



Les agents du réseau client s'enregistrent auprès du serveur de modularité. Le serveur de modularité se connecte au gestionnaire de domaine dans le réseau sous-traitant via une connexion de passerelle ENC. Les étapes de déploiement sont très similaires au scénario pour la petite entreprise, à l'exception de la configuration de l'agent. Dans ce scénario, les agents DSM sont configurés pour s'enregistrer auprès du serveur de modularité "interne".

Dans ce scénario de sous-traitant de taille moyenne, ENC ne se trouve généralement pas sur les points d'arrivée. Dans ce cas, cela signifie que les connexions directes ne fonctionneront pas, sauf si ENC est configuré et exécuté sur les points d'arrivée. Les connexions directes sont utilisées pour les communications suivantes :

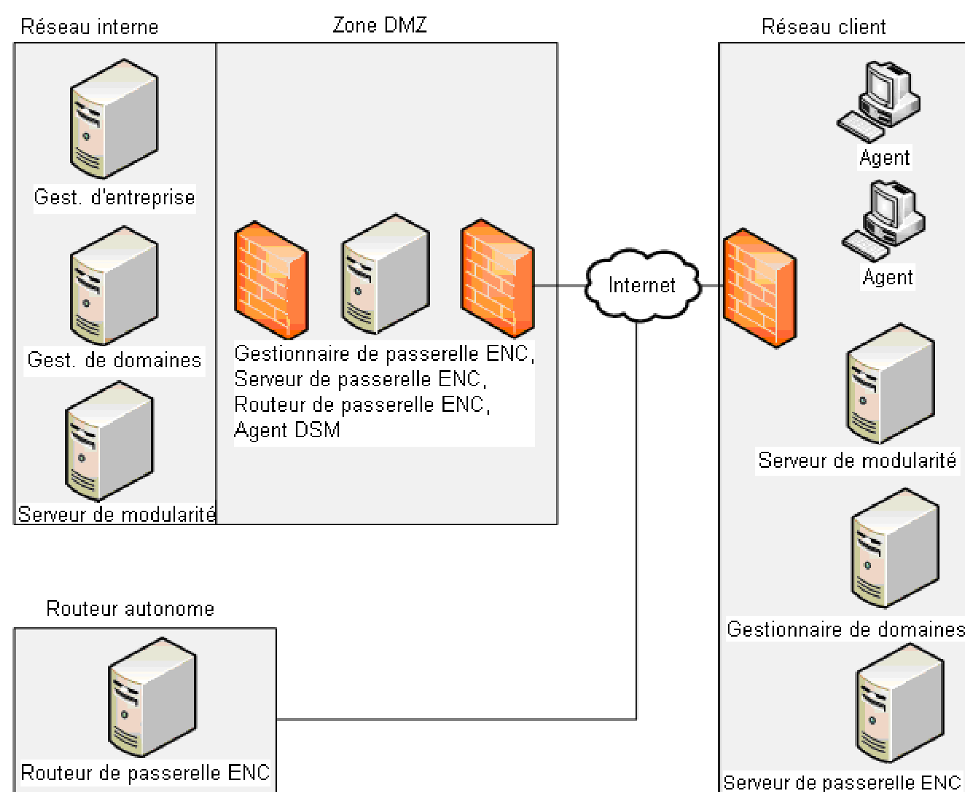
- Hôte Remote Control - affichage de la connexion
- Diagnostic instantané de l'explorateur DSM vers l'agent
- Catalogue de logiciels de l'agent vers le gestionnaire
- Notifications DTS

Scénario de déploiement ENC - Grande entreprise cliente sous-traitante

Dans ce scénario, l'entreprise est suffisamment grande pour posséder son propre gestionnaire de domaine ainsi qu'un certain nombre de serveurs de modularité et un serveur de passerelle ENC.

La compagnie sous-traitante entretient un gestionnaire d'entreprise qui doit être lié au gestionnaire de domaine du client.

L'illustration suivante présente la configuration réseau dans un exemple de scénario de déploiement de la passerelle ENC dans une grande entreprise cliente sous-traitante :



Une fois le gestionnaire de domaine client installé, celui-ci peut être utilisé pour déployer les agents DSM, comme dans le client.

La stratégie peut être configurée localement à l'aide du gestionnaire de domaine du client afin d'autoriser le serveur de passerelle ENC à accepter les connexions ENC des ordinateurs du client.

Le gestionnaire d'entreprise réplique sa base de données sur le gestionnaire de domaine en utilisant le fournisseur de base de données lui-même. Cela est impossible via une connexion de la passerelle ENC. Pour y remédier, les pare-feux doivent être configurés comme décrit dans la meilleure pratique Microsoft ou Oracle publiée.

Les ordinateurs de l'entreprise sous-traitante doivent pouvoir se connecter aux ordinateurs du client. Cela nécessite la configuration du gestionnaire de passerelle ENC du sous-traitant avec les règles d'autorisation qui permettent les opérations suivantes :

- Connexions à partir du serveur de passerelle ENC du client
- Enregistrement des ordinateurs dans le réseau client
- Connexions des ordinateurs du réseau client aux ordinateurs du réseau sous-traitant, et inversement

Routeurs de passerelle ENC autonomes

Des routeurs de passerelle ENC supplémentaires peuvent également être déployés pour des questions de résilience ou de modularité. Ces routeurs de passerelle ENC peuvent être installés ailleurs sur Internet ou dans les succursales.

Les étapes de déploiement pour les routeurs de passerelle ENC autonomes sont les suivantes :

- Installez un agent DSM et un routeur de passerelle ENC et configurez-les pour s'enregistrer auprès du serveur de passerelle ENC dans le bureau sous-traitant. Le routeur peut naturellement être configuré pour s'enregistrer auprès d'un autre serveur de passerelle ENC adapté.
- Au niveau du gestionnaire de domaine, ajoutez les règles d'autorisation adaptées à la stratégie prévue pour l'ordinateur du routeur autonome. Les règles doivent autoriser le routeur dans le domaine dans lequel il réside à se connecter à s'enregistrer.
- Installez un certificat correspondant sur l'ordinateur du routeur.
- Démarrez Client Automation sur l'ordinateur du routeur. Le routeur doit ensuite s'enregistrer auprès du serveur de passerelle ENC. Vérifiez le journal des événements à ce sujet.

  Remarque : Pour afficher ces événements, vous devez définir le paramètre de configuration itrm/common/enc/audit/enabled sur 1. Dans la stratégie de configuration, cela apparaîtra sous la forme "Activer tout". Cela active l'audit de tous les événements ENC. Cela vous permet de voir plus clairement l'activité dans le système ENC. Par défaut, seuls ces événements dans la catégorie "erreur" sont activés. Pour restaurer l'audit à la normal, définissez le paramètre de configuration sur 2 ("Activer par catégorie").
- Une fois le client ENC enregistré sur l'ordinateur du routeur, l'infrastructure Client Automation pourra accepter la stratégie et ainsi installer les règles d'autorisation pour le routeur. Lorsque le routeur a sélectionné les règles d'autorisation, il pourra jouer le rôle de routeur auquel les autres ordinateurs du réseau de passerelle ENC se connectent.

Serveurs de passerelle ENC autonomes

Des considérations similaires aux routeurs de passerelle ENC s'appliquent aux serveurs de passerelle ENC autonomes. La différence réside dans les règles d'autorisation qui correspondent à un rôle de serveur, c'est-à-dire qu'elles autorisent les opérations qu'un serveur de passerelle peut effectuer, contrairement à celles qu'un routeur de passerelle peut effectuer.

Prise en charge du proxy Internet

Si le chemin d'un client ENC vers un serveur de passerelle ENC est bloqué par un proxy Internet, il doit être configuré pour se connecter via ce proxy. La passerelle ENC prend en charge les proxy SOCKS4, SOCKS5 et HTTP. L'authentification peut être configurée par un nom d'utilisateur explicite et un mot de passe ou l'emprunt de l'utilisateur connecté. Le client peut également utiliser les paramètres Internet Explorer actuels pour localiser le proxy.

Les propriétés à définir sont localisées dans le noeud de stratégie "common components/enc/client".

Pour configurer un proxy SOCKS, configurez les paramètres de la manière suivante :

- SocksProxyAddress et SocksProxyPort pour identifier l'ordinateur du proxy
- SocksProxyAuthType pour définir le type d'authentification à utiliser (de base ou sécurisée)
- SocksProxyImpersonate, qui permet au client d'utiliser les informations de connexion de l'utilisateur connecté. Cela signifie évidemment que le client ne peut pas se connecter, sauf si quelqu'un est connecté.
- SocksProxyUsername et SocksProxyPassword, si vous souhaitez utiliser des informations de connexion explicites pour vous authentifier auprès du proxy
- SocksProxyDiscovery, si vous souhaitez que le client ENC localise automatiquement le proxy à l'aide des paramètres IE. Dans ce cas, vous aurez généralement défini le paramètre SocksProxyImpersonate

Pour configurer un proxy HTTP, configurez les mêmes paramètres, sauf que "HTTP" remplace "Socks" dans les noms de paramètres.

Remarque : La configuration du proxy peut également être définie à l'aide de l'utilitaire encUtilCmd. Cela peut s'avérer utile lorsque l'ordinateur en question est déconnecté de la stratégie gérée par le pare-feu mais requiert manifestement des paramètres de stratégie pour pouvoir se connecter.

Restrictions de l'utilisation de Client Automation via une passerelle ENC

Il existe un certain nombre de restrictions appliquées aux fonctions de CA Client Automation (Client Automation) lorsqu'elles sont utilisées via une connexion de passerelle ENC. Ces restrictions sont les suivantes :

- Wake-on-LAN (WOL) ne peut pas fonctionner via une passerelle ENC car celle-ci prend uniquement en charge les connexions TCP, tandis que WOL utilise UDP.
- Certaines fonctions de diagnostics instantanés ne fonctionnent pas du fait qu'elles s'appuient sur des composants fournis par le système d'exploitation et ne connaissant pas la passerelle ENC, par exemple FTP.
- L'emplacement de service ne peut pas fonctionner car il utilise UDP.
- Le générateur de rapports ne peut pas fonctionner car il accède directement à la MDB.
- Les jobs Software Delivery (SD) via la passerelle ENC peuvent prendre jusqu'à 10 minutes pour être déclenchés. Cela est dû au fait que SD tentera d'utiliser l'adresse IP de la cible lorsqu'elle s'enregistre, mais cela échouera car les adresses IP ne sont pas valides sur différents réseaux. Le serveur de modularité SD essayera à nouveau le job toutes les 10 minutes, en alternant entre le FQN et l'IP de la cible. Le FQN fonctionnera avec la passerelle ENC car il utilise le FQN des ordinateurs sur lesquels la passerelle ENC est activée afin de les identifier de manière unique.
- Certains composants de Client Automation utilisent des composants SQL Server ou Oracle côté client pour établir des connexions directes à la base de données de gestion (MDB). Ces connexions n'ont pas l'ENC activé, de sorte que vous devez utiliser la méthode Microsoft ou Oracle recommandée de traversée du pare-feu si ces connexions passent par des pare-feux.

  La liste suivante détaille les scénarios et les composants DSM auquel un accès direct à la MDB est établi, ainsi que les composants spécifiques au côté client utilisés pour SQL Server et Oracle :

  - **Gestionnaire de domaine depuis et vers le gestionnaire d'entreprise**

    La réplication de la MDB entre le gestionnaire de domaine et le gestionnaire d'entreprise utilise les connexions directes et les copies en bloc.

    Composants côté client :

    Pour SQL Server : SQL Native Client et Utilitaire bcp

    Pour Oracle : OCI API et SQL*Loader

- **Moteur vers le gestionnaire de domaine et le gestionnaire d'entreprise**

  Le moteur établit les connexions vers la base de données lors de la communication avec le gestionnaire de domaine et le gestionnaire d'entreprise.

  Composants côté client :

  Pour SQL Server : SQL Native Client et Utilitaire bcp

  Pour Oracle : OCI API et SQL*Loader

- **Générateur de rapports vers le gestionnaire de domaine ou le gestionnaire d'entreprise**

  Le générateur de rapports établit des connexions directes pour générer des rapports.

  Composants côté client :

  Pour SQL Server : SQL Native Client et Utilitaire bcp

  Pour Oracle : OCI API et SQL*Loader

- **Console Web vers le gestionnaire de domaine ou le gestionnaire d'entreprise**

  Le composant Console Web établit une connexion JDBC vers la base de données.

  Composants côté client :

  Pour SQL Server : JDBC

  Pour Oracle : JDBC

- **Utilitaire d'importation/exportation de contenu**

  L'Utilitaire d'importation/exportation de contenu établit des connexions directes à la base de données lors de la synchronisation des données DSM avec une MDB Oracle ou SQL Server distante.

  Composants côté client :

  Pour SQL Server : SQL Native Client et Utilitaire bcp

  Pour Oracle : OCI API et SQL*Loader

Utilisation de l'utilitaire encUtilCmd

L'utilitaire encUtilCmd est un programme conçu pour implémenter différentes fonctions de l'utilitaire Passerelle ENC. Cependant, cette section traite seulement un cas d'utilisation de encUtilCmd.

Pour la description détaillée de la commande encUtilCmd et toutes ses options, consultez le document *Référence de la commande encUtilCmd* que vous trouverez dans la bibliothèque CA, dans la catégorie Manuels de référence.

L'utilitaire encUtilCmd combiné à d'autres fonctionnalité gèrera le problème de configuration de la sécurité de la passerelle ENC.

Ce cas d'utilisation traite un problème survenant après l'installation d'un serveur de modularité, en état verrouillé. Le gestionnaire de domaine ne parvient pas à établir une connexion directe au serveur de modularité en raison de la présence d'un pare-feu. Cette méthode ne peut donc pas être utilisée pour transmettre la stratégie au serveur de modularité. Le gestionnaire de domaine ne peut pas utiliser la passerelle ENC pour contacter le serveur de modularité du fait que celui-ci rejettera toutes les tentatives de connexion. Cette stratégie définit qui peut se connecter au serveur de modularité.

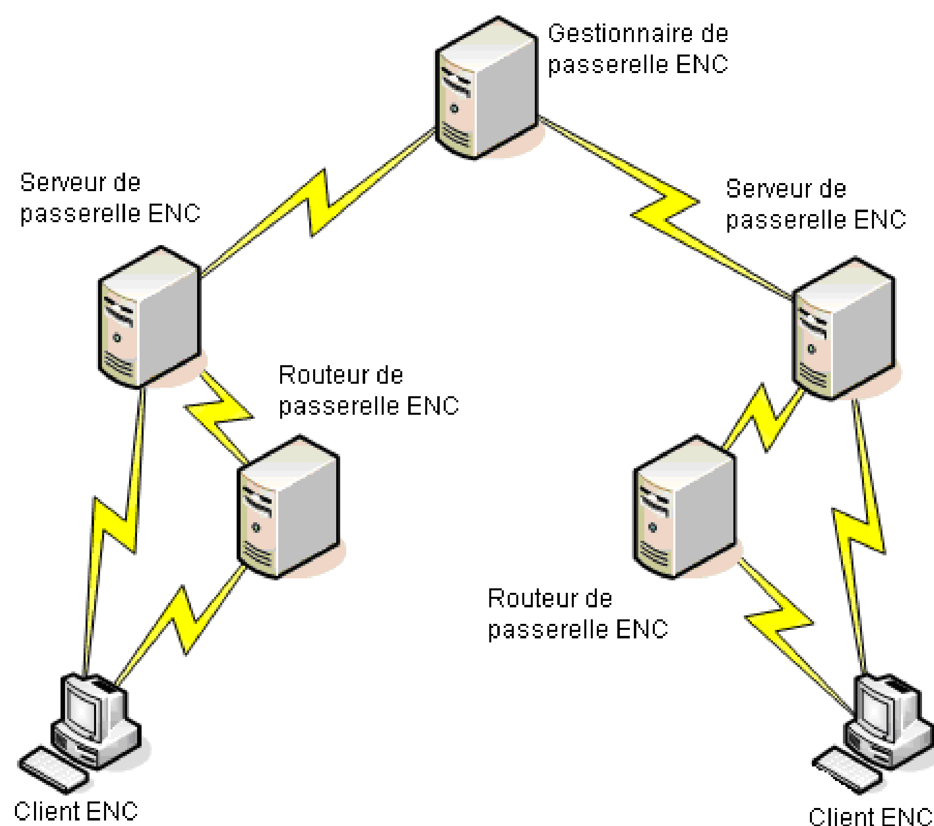
Pour résoudre ce problème, vous pouvez définir des règles dans un fichier texte et l'importer sur le serveur de passerelle ENC à l'aide de la commande encUtilCmd.

Gestion des certificats

Dans l'infrastructure de Connectivité de réseau étendu (ENC), toutes les communications entre les noeuds sont sécurisées à l'aide du protocole standard de sécurité de la couche de transport (TLS). Ce protocole offre confidentialité, intégrité et authentification mutuelle.

La portion d'authentification du protocole TLS est fournie par l'utilisation de certificats numériques et de la cryptographie de la clé publique. La confidentialité est générée par la cryptographie de clé symétrique.

L'illustration suivante présente les connexions entre les noeuds entre les composants ENC dans une infrastructure ENC.



Toutes les connexions entre les noeuds dans l'infrastructure ENC sont protégés par l'authentification TLS. L'authentification est toujours mutuelle : l'initiateur d'une connexion s'authentifie auprès du répondeur et ce dernier s'authentifie auprès de l'initiateur. Cela permet à l'infrastructure ENC de valider les ordinateurs qui s'y connectent et aux clients ENC d'être en confiance avec les ordinateurs auxquels ils se connectent.

Certificats X.509

La connectivité du réseau étendu (ENC) utilise les certificats numériques X.509 version 3 pour l'authentification. Le profil du certificat utilisé est celui de l'implémentation RFC 3280 du groupe de travail IETF PKIX.

Les certificats et leurs clés privées associées sont obtenues via le magasin de certificats Microsoft. Les certificats doivent posséder une extension Enhanced Key Usage marquée pour l'authentification du serveur (1.3.6.1.5.5.7.3.1) ou l'authentification du client (1.3.6.1.5.5.7.3.2), en fonction de l'application qui l'utilise.

Une extension Client Automation privée à l'extension du certificat Enhanced Key Usage peut être utilisée pour aider à localiser le certificat (1.3.6.1.4.1.791.2.10.8.3). Cet identificateur de l'objet (OID) est privé pour CA Technologies et est interne à l'arborescence CA OID.

Aucune limite ENC n'est imposée à la taille de la clé RSA utilisée dans la paire de clés du certificat. La taille des clés utilisées est un choix spécifique à l'organisation, mais nous vous recommandons une clé d'un minimum de 1024 bits.

Gestion des certificats à l'aide de l'infrastructure PKI

La création et la distribution des certificats peut s'avérer être un processus difficile. L'utilisation de l'infrastructure de clés publiques (PKI) pour automatiser et augmenter ce processus est fortement recommandée.

Exigences relatives aux certificats

La passerelle ENC utilise les certificats X.509 v3 émis pour être utilisés par le protocole de sécurité standard TLS 1.0 (SSL3.1). La passerelle ENC peut utiliser les certificats TLS standard, mais prend également en charge une extension Extended Key Usage pour autoriser le sous-système ENC à identifier les certificats essentiellement utilisés par la passerelle ENC.

La passerelle ENC recherche le meilleur certificat à charger pour son identité. Lors du premier passage, elle recherche les certificats valides (avec les clés privées associées) marqués par l'extension de l'utilisation CA ENC (voir (1) dans le tableau suivant) ainsi que l'extension de l'utilisation TLS pour l'authentification client (2) ou l'authentification serveur (3), respectivement.

Le tableau ci-dessous fournit des détails supplémentaires sur les termes marqués de (1) à (4) dans le paragraphe précédent :

Marqueur	Informations
(1)	CA Technologies a attribué en interne un identificateur de l'objet (OID) à utiliser dans les certificats X.509 v3 sous forme d'identificateur Enhanced Key Usage (voir RFC2459 section 4.2.1.13). Cet OID indique que le certificat est à utiliser par le sous-système de sécurité ENC. ■ L'identificateur de l'objet est "1.3.6.1.4.1.791.2.10.8.3" ■ La balise des identificateurs de l'objet est "OID_PKIX_KP_CA_CMS_ENC_TLS_AUTH" ■ L'extension d'utilisation peut être marquée comme critique ou non critique. ■ L'OID de base CA Technologies est "1.3.6.1.4.1.791" enregistré par l'IANA.
(2)	L' OID de l'authentification du client TLS est "1.3.6.1.5.5.7.3.2"
(3)	L' OID de l'authentification du serveur TLS est "1.3.6.1.5.5.7.3.1"
(4)	Pour les noeuds de passerelle ENC qui servent à la fois de client et de serveur (routeurs et serveurs de passerelle), le sous-système de sécurité peut utiliser un certificat unique marqué pour l'authentification client et serveur, ou des certificats individuels marqués comme authentification client uniquement et authentification serveur uniquement, respectivement.

Si la passerelle ENC ne trouve pas les certificats appropriés, elle répète la recherche sans l'exigence de l'extension d'utilisation CA ENC.

Lorsque vous créez des certificats utilisés par la passerelle ENC, nous vous recommandons d'ajouter l'OID d'utilisation de clé étendue CA aux certificats ; toutefois, la passerelle ENC fonctionnera également sans.

L'identificateur de l'objet d'authentification privé pour CA Technologies

Une extension Client Automation privée à l'extension du certificat Enhanced Key Usage peut être utilisée pour aider à localiser le certificat (1.3.6.1.4.1.791.2.10.8.3).

Cet identificateur de l'objet (OID) est privé pour CA Technologies et est interne à l'arborescence CA Technologies OID.

Chapitre 13: Intégration à CA Service Desk Manager

L'intégration de CA Client Automation à CA Service Desk Manager fait de CA Client Automation une application Service Aware, ce qui signifie que CA Client Automation peut se déclencher sur certains événements de ses ressources gérées et créer des tickets dans CA Service Desk Manager.

La création de ticket et le flux de travaux dans CA Service Desk Manager est contrôlée par la stratégie Service Aware qui énumère une liste de types de problèmes. CA Client Automation utilise les types de problèmes pour classer le problème et déterminer le type de ticket à créer.

CA Client Automation et CA Service Desk Manager proposent des interfaces utilisateur graphiques permettant le démarrage contextuel de l'un et de l'autre pour l'intégration.

Ce chapitre décrit l'installation et la configuration du système, ainsi que les aspects de la sécurité et de l'authentification. Les observations relatives à la configuration s'appliquent aux gestionnaires de domaine et d'entreprise DSM.

Pour plus de détails sur CA Service Desk Manager, comme les types de problème, reportez-vous à la documentation d'CA Service Desk Manager.

Ce chapitre traite des sujets suivants :

Stratégie Service Aware

En ce qui concerne l'intégration de Client Automation à CA Service Desk Manager, la stratégie Service Aware portant le nom ManagedAssetEvents est définie. La stratégie Service Aware est automatiquement installée lors de l'installation de CA Service Desk Manager. Client Automation utilise les types de problème disponibles avec la stratégie lors de la création des tickets.

Les principaux paramètres de la stratégie Service Aware se présentent comme suit :

Afficher le nom:

Evénements d'actifs gérés

Code :

MANAGED_ASSET_EVENTS

Description :

Cette stratégie Service Aware est utilisée pour traiter des tickets en cours de déclenchement par les actifs gérés via les services Web.

En plus des types de problème par défaut de CA Service Desk Manager, la stratégie Service Aware comporte les types de problème répertoriés dans le tableau suivant. Les administrateurs CA Service Desk Manager peuvent modifier ces types de problème ou ajouter leurs propres types de problème à cette liste.

Afficher le nom du type de problème	Code du type de problème	Description du type de problème	Priorité (5 est la plus élevée)
Stratégie basée sur les événements d'actifs (élevée)	ASSET_EVENT_ POLICY_H	Un actif géré a rencontré une violation de stratégie utilisant des événements avec une priorité élevée.	4
Stratégie basée sur les événements d'actifs (moyenne)	ASSET_EVENT_ POLICY_M	Un actif gérée a rencontré une violation de stratégie utilisant des événements avec une priorité moyenne.	3
Stratégie basée sur les requêtes d'actifs (élevée)	ASSET_QUERY_ POLICY_H	Un actif géré a rencontré une violation de stratégie basée sur les requêtes avec une priorité élevée.	4
Stratégie basée sur les requêtes d'actifs (moyenne)	ASSET_QUERY_ POLICY_M	Un actif géré a rencontré une violation de stratégie basée sur les requêtes avec une priorité moyenne.	3

Afficher le nom du type de problème	Code du type de problème	Description du type de problème	Priorité (5 est la plus élevée)
Echec de la distribution de logiciels (élevée)	SW_DISTR_FAIL _H	Un job Software Delivery a échoué avec une priorité élevée.	4
Echec de la distribution de logiciels (moyenne)	SW_DISTR_FAIL _M	Un job Software Delivery a échoué avec une priorité moyenne.	3
Echec de la distribution de logiciels (faible)	SW_DISTR_FAIL _L	Un job Software Delivery a échoué avec une faible priorité.	2

Gestion des tickets

Des tickets peuvent être créés au niveau du domaine et de l'entreprise. Les événements suivants peuvent entraîner la création d'un ticket :

- Une violation de la stratégie s'est produite.
- Un job Software Delivery a échoué.
- Un administrateur crée un ticket de façon interactive via un menu contextuel dans le cadre d'un ordinateur.

Afin d'éviter l'inondation de tickets, les règles suivantes restreignent la création de nouveaux tickets :

- Un seul ticket est créé pour chaque stratégie. Un ticket est créé lorsque la première violation de stratégie se produit. Pour chaque nouvelle violation de la même stratégie, un journal est ajouté au ticket.
- Un seul ticket est créé pour chaque job logiciel. Un ticket est créé lorsque le premier échec du job logiciel se produit. Pour chaque nouvel échec du même job logiciel, un journal est ajouté au ticket.

Pour plus d'informations sur la gestion des tickets, reportez-vous à la documentation d'CA Service Desk Manager.

Association des ressources détectées et des ressources détenues

Client Automation crée des tickets dans le contexte des ressources détectées, comme des ordinateurs ou des utilisateurs. Lorsqu'un ticket est créé, une ressource détectée est mappée vers une ressource détenue, connue dans CA Service Desk Manager. Cela permet aux administrateurs CA Service Desk Manager de naviguer et de consigner la relation entre des tickets et des ressources détenues.

Lancement en contexte entre Client Automation et CA Service Desk Manager

Le tableau suivant fournit un aperçu des lancements en contexte pris en charge entre l'explorateur DSM ou la console Web DSM et l'interface utilisateur graphique Web CA Service Desk Manager.

De	A	Dans le contexte de	Contexte
Explorateur / Console Web	Interface utilisateur graphique Web CA Service Desk Manager	Job logiciel	Ticket créé lors de l'échec du job
Explorateur / Console Web	Interface utilisateur graphique Web CA Service Desk Manager	Stratégie Actif	Ticket créé lors de la violation d'une stratégie
Interface utilisateur graphique Web CA Service Desk Manager	Explorateur / Console Web	Détails du ticket	Job logiciel
Interface utilisateur graphique Web CA Service Desk Manager	Explorateur / Console Web	Détails du ticket	Stratégie Actif

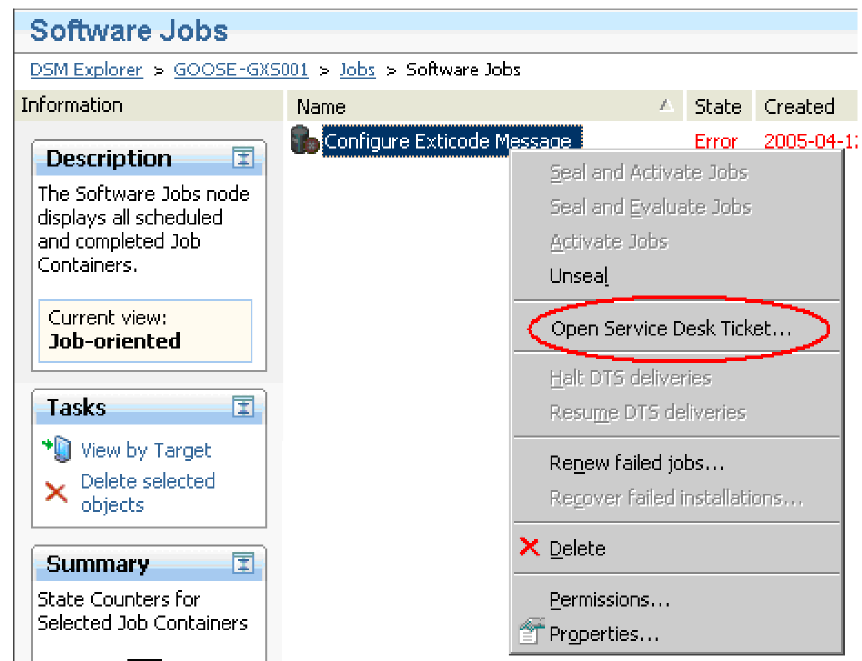
Lancement en contexte de Client Automation vers CA Service Desk Manager

Client Automation propose des interfaces utilisateur qui vous permettent de lancer CA Service Desk Manager dans le contexte suivant :

- d'un échec du job logiciel (page 517),
- d'une violation de la stratégie Asset (page 518).

Détails du ticket dans le contexte d'un échec du job logiciel

Les jobs logiciels ayant échoué et entraîné un ticket CA Service Desk Manager proposent une entrée de menu contextuel Ouvrir un ticket Service Desk que vous pouvez afficher en cliquant avec le bouton droit de la souris sur le job de sauvegarde échoué. Si vous sélectionnez Ouvrir un ticket Service Desk, l'interface utilisateur graphique CA Service Desk Manager est lancée.

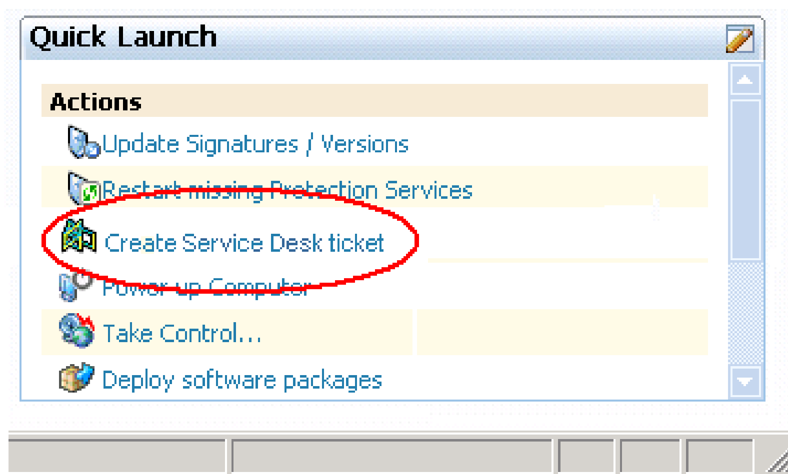


Détails du ticket dans le contexte d'une violation de la stratégie Asset

Lorsqu'une stratégie est activée pour CA Service Desk Manager, le lien hypertexte Ouvrir un ticket Service Desk connexe apparaît dans la colonne Information de l'explorateur DSM. En sélectionnant ce lien hypertexte, vous lancez l'écran des détails du ticket CA Service Desk Manager de ce ticket, qui a été généré à l'origine par une violation de cette stratégie.

Création de ticket dans le contexte d'une ressource gérée (ad hoc)

Les tickets CA Service Desk Manager sont créés de façon interactive en cliquant sur l'action Créer un ticket Service Desk dans le portlet de lancement rapide :



Le portlet de lancement rapide est situé sur l'onglet Page d'accueil qui s'ouvre quand vous sélectionnez la ressource gérée dans l'explorateur DSM.

La méthode Créer un ticket est également disponible en tant que commande dans le menu contextuel de ressources.

Lancement en contexte d'CA Service Desk Manager vers Client Automation

L'Explorateur DSM et la console Web sont lancés depuis l'interface utilisateur graphique Web de CA Service Desk Manager par le biais d'URL individuelles.

Le lien hypertexte, qui lance l'explorateur DSM ou la console Web DSM, s'affiche dans le champ Description des informations récapitulatives du ticket CA Service Desk Manager :

Summary Information

Summary			Total Activity Time
Asset Event-based Policy high			00:00:00
Description			
2007-04-12 10:06 - GOOSE-GXS001 :: goose-gxs001 violated policy 'Test'			
Open Date/Time	**Last Modified**	**Resolve Date/Time**	**Close Date/Time**
04/12/2007 10:06 am	04/12/2007 10:06 am		

Remarque : Comme l'explorateur DSM est lancé grâce à la commande dsmgui.exe, il doit être installé sur l'ordinateur CA Service Desk Manager exécutant l'interface utilisateur graphique Web de CA Service Desk Manager.

Installation d'CA Service Desk Manager et de Client Automation

L'installation d'CA Service Desk Manager installe automatiquement la stratégie Service Aware pour Client Automation et les types de problème prédéfinis pour la création de tickets. Le nom de la stratégie Service Aware est ManagedAssetEvents. Les types de problème prédéfinis peuvent être modifiés ou améliorés à tout moment par l'administrateur CA Service Desk Manager.

En outre, CA Service Desk Manager crée un compte de proxy pour Client Automation, System_MA_User, configuré avec un ensemble défini de privilèges, puis l'associe à la stratégie Service Aware.

L'installation de Client Automation crée automatiquement une stratégie de configuration pour l'intégration à CA Service Desk Manager. La stratégie de configuration est installée sur le gestionnaire de configuration commune (CCNF) sous le nom de chemin suivant :

```
/Default Computer Policy/DSM/Service Desk Integration/default
```

Pour activer l'intégration, l'administrateur Client Automation doit installer la stratégie de configuration en utilisant l'interface utilisateur graphique du gestionnaire de configuration commune.

Les paramètres de la stratégie de configuration englobent les domaines suivants :

- Un commutateur indiquant si l'intégration d'CA Service Desk Manager est activée.
- Des paramètres de connexion sécurisée au Service Web CA Service Desk Manager.
- L'URL pour accéder au Service Web CA Service Desk Manager.

Condition préalable au lancement en contexte d'CA Service Desk Manager

L'intégration de CA Service Desk Manager prend en charge les lancements sensibles au contexte depuis l'explorateur DSM vers l'interface utilisateur graphique Web CA Service Desk Manager. Ces lancements impliquent que vous disposiez des autorisations d'accès appropriées dans CA Service Desk Manager. Ainsi, le compte utilisateur (ID utilisateur et mot de passe) avec lequel vous êtes connecté à l'explorateur DSM doit également être créé comme un contact dans CA Service Desk Manager.

Si votre compte utilisateur Client Automation est inconnu dans CA Service Desk Manager, un écran de connexion s'affiche lorsque vous tentez de lancer l'interface utilisateur graphique Web CA Service Desk Manager.

Conditions préalables à l'intégration d'CA Service Desk Manager à plusieurs moteurs

Si vous utilisez plusieurs moteurs pour évaluer les stratégies, l'intégration d'CA Service Desk Manager doit être activée pour tous les systèmes sur lesquels s'exécute un moteur, ce qui signifie que les conditions préalables suivantes doivent être remplies sur chaque système :

- Un agent est installé et en cours d'exécution.
- La stratégie de configuration qui active l'intégration d'CA Service Desk Manager a été glissée-déplacée sur cet agent.
- Le fichier de certificat .p12 est importé (si la méthode gérée est utilisée).

Conditions préalables à l'intégration d'CA Service Desk Manager au gestionnaire d'entreprise

Pour activer l'intégration d'CA Service Desk Manager sur le gestionnaire d'entreprise, les conditions préalables suivantes doivent être remplies sur le gestionnaire d'entreprise :

- Un agent connecté à l'un des gestionnaires de domaines liés est installé et en cours d'exécution.
- La stratégie de configuration qui active l'intégration d'CA Service Desk Manager a été glissée-déplacée sur cet agent.
- Le fichier de certificat .p12 est importé (si la méthode gérée est utilisée).

A propos de l'intégration de Client Automation et d'CA Service Desk Manager

Il est important de tenir compte des observations suivantes, car elles risquent d'affecter vos scénarios d'intégration de Client Automation et d'CA Service Desk Manager :

- Job Software Delivery d'un gestionnaire d'entreprise activé pour Service Desk (page 522)

Job Software Delivery d'un gestionnaire d'entreprise activé pour Service Desk

Les éléments ci-dessous s'appliquent au scénario où l'intégration de Client Automation et d'CA Service Desk Manager est effectuée sur un gestionnaire d'entreprise.

Un job Software Delivery démarré depuis le gestionnaire d'entreprise activé pour Service Desk ne crée pas de ticket Service Desk, il échoue en raison de modules d'extension DTS arrêtés sur le gestionnaire d'entreprise ou le gestionnaire de domaines.

Connexion sécurisée au Service Web CA Service Desk Manager

L'administrateur Client Automation peut faire son choix entre deux méthodes de connexion sécurisée au service Web CA Service Desk Manager :

- une méthode de connexion simple qui requiert un nom d'utilisateur et un mot de passe (méthode non gérée)
- une méthode de connexion gérée utilisant des clés publiques/privées et un chiffrement eTrust PKI

L'authentification par nom d'utilisateur/mot de passe et par clés publiques/privées ne sont pas disponibles immédiatement. Une étape distincte de configuration est requise après l'installation réussie de CA Service Desk Manager et Client Automation.

La méthode de connexion sécurisée est spécifiée grâce au paramètre sdlogonmanaged dans la stratégie de configuration Client Automation (comstore). La valeur par défaut de ce paramètre est Géré, ce qui signifie que la connexion se produit grâce à un certificat et à un chiffrement/ déchiffrement basé sur PKI eTrust. La valeur Non géré signifie que l'utilisateur ouvre une session en utilisant un nom d'utilisateur et un mot de passe.

Comment configurer la connexion sécurisée

Pour configurer la connexion sécurisée, l'administrateur Client Automation doit effectuer les étapes de configuration suivantes :

1. Sélectionnez la méthode d'authentification.
2. Si vous choisissez la méthode non gérée, effectuez les actions suivantes :
   - Créez un système d'exploitation respectif pour CA Service Desk Manager.
   - Configurez Client Automation en conséquence, grâce à une stratégie de configuration.
3. Si vous choisissez la méthode gérée, effectuez les actions suivantes :
   - Créez un certificat X.509 avec une clé privée et exposez-le avec un fichier PKCS#12. Pour ce faire, les administrateurs peuvent utiliser l'utilitaire CA Service Desk Manager pdm_pki ou fournir leurs propres certificats.
   - Importez le fichier de stratégie créé dans Client Automation avec l'utilitaire Client Automation cacertutil.

Méthode par nom d'utilisateur et mot de passe (non gérée)

Les paramètres sdusr et sdpwd de la stratégie de configuration sont utilisés respectivement pour le nom d'utilisateur et le mot de passe.

L'installation d'CA Service Desk Manager charge automatiquement le contact System_MA_User utilisé par Client Automation et l'associe à la stratégie Service Aware Client Automation ManagedAssetEvents.

En d'autres termes, la valeur par défaut de sdusr est System_MA_User.

Pour activer le nom d'utilisateur et le mot de passe comme méthode de connexion, l'administrateur CA Service Desk Manager doit effectuer les actions suivantes :

- Créer un utilisateur du système d'exploitation.
- Modifier le contact du System_MA_User et placer le nom d'utilisateur du système d'exploitation dans le champ Connexion système

  (Par défaut, la connexion système est égale à System_MA_User).

L'administrateur Client Automation doit mettre à jour la stratégie de configuration Client Automation avec le nom du contact et le mot de passe correspondants, créés dans CA Service Desk Manager.

Les administrateurs sont autorisés à créer et à utiliser un contact différent de System_MA_User. Ainsi, ils doivent modifier la configuration dans CA Service Desk Manager et la stratégie de configuration Client Automation de façon synchrone.

Méthode par certificat ou PKI eTrust (gérée)

L'installation d'CA Service Desk Manager charge automatiquement le contact System_MA_User utilisé par Client Automation et associe ce contact à la stratégie Service Aware Client Automation ManagedAssetEvents.

Pour utiliser le certificat (eTrust PKI) comme méthode de connexion, l'administrateur CA Service Desk Manager doit suivre deux étapes :

- Créer un fichier PKCS#12 (page 524).
- Importer le fichier PKCS#12 dans le fichier de configuration Client Automation (page 525).

Créer un fichier PKCS#12

Les administrateurs peuvent fournir leurs propres clés par le biais d'un fichier PKCS#12. Par exemple, l'administrateur peut utiliser des autorités de certification tierces à cette fin.

Pour créer un fichier PKCS#12, procédez comme suit à l'aide de l'utilitaire (commande) CA Service Desk Manager pdm_pki :

1. Créez une paire de clés publique/ privée.
2. Associez la clé publique à la stratégie Client Automation dans la base de données CA Service Desk Manager.
3. Créez un certificat X.509 avec la clé privée et exposez-le avec un fichier PKCS#12.

L'utilitaire pdm_pki crée un fichier PKCS#12 dans son répertoire de travail avec le nom de fichier MANAGED_ASSET_EVENTS.p12.

La commande pdm_pki a le format suivant :

```
pdm_pki -p MANAGED_ASSET_EVENTS [-l certificate_file] [-f]
```

-p

Définit le code de la stratégie. Dans ce cas, la valeur MANAGED_ASSETS_EVENTS doit être utilisée.

-l

Charge un certificat à partir d'un fichier au lieu d'en créer un nouveau.

-f

Force le remplacement d'une clé existante.

Importation du fichier PKCS#12 dans le fichier de configuration Client Automation

Pour importer le fichier PKCS#12 dans le fichier de configuration Client Automation (comstore), utilisez l'utilitaire Client Automation cacertutil comme décrit ci-dessous.

La commande cacertutil, permettant d'importer le fichier PKCS#12 dans le fichier de configuration Client Automation (comstore), a le format suivant :

```
cacertutil import -i:certificate_file
    -ip:MANAGED_ASSET_EVENTS -t:MANAGED_ASSET_EVENTS
    -l:global
```

-i

Identifie le nom de fichier du certificat.

-ip

Identifie la phrase de passe.

-t

Spécifie la balise d'identité.

-l

Identifie l'utilisateur.

Paramètres dans la stratégie de configuration

Les paramètres de configuration pour l'intégration de CA Service Desk Manager sont spécifiés dans la section des paramètres sdintegration du fichier de configuration Client Automation (comstore.xml). Les paramètres du fichier de configuration sont définis pour être gérés de façon centralisée via une stratégie de configuration commune (CCNF).

Les paramètres suivants sont utilisés pour l'intégration de CA Service Desk Manager.

SdIsEnabled

Indique si l'intégration de CA Service Desk Manager est activée. Si la valeur de SdIsEnabled est True, l'intégration de CA Service Desk Manager est activée. Si la valeur est False, l'intégration n'est pas activée.

Valeur par défaut : False

SdEnd

Identifie l'URL pour accéder au service Web CA Service Desk Manager.

Valeur par défaut : http://*monhôte*:8080/axis/services/USD_R11_WebService

Remplacez *monhôte* par l'adresse de serveur appropriée à votre service Web CA Service Desk Manager. Le port par défaut est 8080.

SdLogonManaged

Indique la manière dont est contrôlée le service Web CA Service Desk Manager. Si la valeur est Géré, la connexion est contrôlée grâce au certificat PKCS#12. Si la valeur est Non géré, la connexion est contrôlée grâce au compte utilisateur et au mot de passe.

Valeur par défaut : Géré

SdUsr

Spécifie le compte utilisateur de connexion au service Web CA Service Desk Manager. Ce paramètre n'est utilisé que lorsque SdLogonManaged est défini sur Non géré.

Valeur par défaut : System_MA_User

SdPwd

Spécifie le mot de passe de connexion au service Web CA Service Desk Manager. Ce paramètre n'est utilisé que lorsque SdLogonManaged est défini sur Non géré.

Remarque : En plus du compte SdUsr, le compte de l'utilisateur actuellement connecté est également important. Lorsqu'un ticket ad hoc est crée à partir de l'IUG de l'explorateur DSM dans le cadre d'un actif géré, ce compte est désigné comme le créateur du ticket dans CA Service Desk Manager. Lorsqu'un ticket est créé dans le cadre d'Asset Management ou de Software Delivery, le créateur du ticket est toujours l'administrateur.

Valeur par défaut : *Vide*

SdPolicy

Identifie le nom de la stratégie Service Aware CA Service Desk Manager à laquelle se connecter. Ce paramètre n'est utilisé que lorsque SdLogonManaged est défini sur Non géré. Un certificat PKCS#12 utilisé avec la connexion gérée inclut déjà une description de la stratégie qui ignorera toujours cette valeur. Si ce paramètre n'est pas spécifié, la stratégie CA Service Desk Manager par défaut est sélectionnée.

Valeur par défaut :MANAGED_ASSET_EVENTS

SdThrottle

Spécifie si la régulation du réseau et de l'UC est activée. Si la valeur est True, la régulation est activée. Si la valeur est False, la régulation est désactivée.

Valeur par défaut : False

SdTimeout

Spécifie l'expiration du délai d'appel pour accéder au service Web CA Service Desk Manager. La valeur peut être modifiée pour forcer une expiration du délai sur envoyer, recevoir et connecter. Les valeurs positives indiquent les secondes avant l'expiration du délai ; par exemple, la valeur 20 indique une temporisation après 20 secondes. Les valeurs négatives indiquent les millisecondes ; par exemple, la valeur -200 indique une expiration du délai après 200 millisecondes.

Valeur par défaut : 0 (Infini)

Chapitre 14: Dépannage

Cette annexe contient les chapitres suivants :

erreur d'annulation de connexion à CIC

Parfois, le service Client d'importation de contenu CA (CIC) peut ne pas parvenir à libérer la connexion à la MDB Oracle, donnant lieu à l'erreur suivante dans le journal du CIC :

```
[CCMain] WARN  [com.ca.sccc.dbm.CCDBManager] - Failed to uninitialize MDB
connection pool for domain 'xxx' (Echec de l'annulation d'initialisation de la
connexion à la MDB pour le domaine xxx)
```

Echec du téléchargement de contenu sur une MDB Oracle

Symptôme :

Un échec du job de téléchargement de contenu se produit sur une MDB Oracle après une nouvelle installation sur le gestionnaire de domaines ou d'entreprise, avec les erreurs suivantes dans les journaux du client d'importation de contenu.

```
ORA-00604: error occurred at recursive SQL level

ORA-01000: maximum open cursors exceeded
```

Solution :

Ce problème survient lors de l'exécution du client d'importation de contenu, si le nombre de curseurs ouverts dépasse la limite maximum définie dans la base de données Oracle.

Vous pouvez remplacer la limite maximale des curseurs ouverts par défaut (50) par une valeur plus élevée.

Exécutez la commande suivante sur la MDB Oracle :

```
ALTER SYSTEM SET open_cursors = 1000 SCOPE=BOTH;
```

Cette commande définit la limite maximale de curseurs ouverts sur 1000.

Remarque : La limite maximale permet d'ouvrir les curseurs requis par le client d'importation de contenu et de les fermer à la fin de l'opération.

Panne du moteur DSM lorsque la base de données est arrêtée

Symptôme :

Lorsque j'arrête la base de données aux fins de maintenance, par exemple pour effectuer une sauvegarde, les processus du moteur s'arrêtent parfois brutal.

Solution :

Avant d'arrêter la base de données aux fins de maintenance, vérifiez que vous avez arrêté tous les processus du moteur.

Remarque : Si un processus de moteur tombe en panne lors de la maintenance de base de données, redémarrez-le après avoir redémarré la base de données.

Configuration requise pour l'outil de packaging SXP sur Windows 8 et 8.1

Si vous avez tenté de créer des packages à l'aide de l'outil de packaging SXP sur l'ordinateur, vérifiez que .NET Framework 3.5 est installée et activée sur l'ordinateur Windows 8 ou Windows Server 2012 à l'aide de la procédure suivante :

Windows 8 et 8.1 :

> Cliquez sur Panneau de configuration, Programmes et fonctionnalités, Activer ou désactiver des fonctionnalités Windows. Pour plus d'informations, consultez l'article http://msdn.microsoft.com/en-us/library/hh506443.aspx.

Windows Server 2012 et Windows Server 2012 R2 :

> Installez .NET Framework 3.5 à l'aide de l'assistant Ajouter des rôles et des fonctionnalités. Pour plus d'informations, consultez l'article http://technet.microsoft.com/en-us/library/hh83180.aspx.

Ouverture des rapports exportés

Les fichiers exportés sont au format Unicode. Pour afficher les fichiers dans une application qui ne prend pas en charge Unicode, modifiez le codage en ANSI avant d'ouvrir le fichier.

Echec de la connexion du collecteur d'alertes au gestionnaire spécifié

Symptôme :

Lorsque vous exécutez la commande status du collecteur d'alertes pendant son installation, le message suivant est renvoyé :

Unable to connect to the specified manager (Impossible de se connecter au gestionnaire spécifié).

Solution :

Lorsque vous installez le collecteur d'alertes sur un serveur autonome configuré pour se connecter au gestionnaire d'entreprise ou au gestionnaire de domaines, il ne parvient pas à s'y connecter. Le collecteur d'alertes se connecte au gestionnaire la première fois pour déterminer le type du gestionnaire (gestionnaire d'entreprise ou gestionnaire de domaines). Lorsqu'un rôle non valide est spécifié, le type de gestionnaire est utilisé pour valider le rôle spécifié et basculer vers le rôle par défaut.

Vérifiez si le CAF est en cours d'exécution et fonctionne sur le serveur autonome et le gestionnaire. Le collecteur d'alertes extrait les informations requises et fonctionne de manière appropriée. Ce message de statut est affiché lorsque le gestionnaire du collecteur d'alertes est modifié et le collecteur d'alertes est relancé. Effectuez les mêmes opérations pour corriger le problème.

Echec de la connexion du collecteur d'alertes à la base de données

Symptôme :

Lors du chargement des alertes vers le collecteur d'alertes, aucune alerte chargée ne s'affiche dans la console d'administration Web à l'aide de la commande *AlertCollector status* et le message suivant s'affiche :

Impossible d'établir une connexion à la base de données

Solution :

Assurez-vous de ce que le collecteur d'alertes sur un serveur autonome se connecte à la base de données, en vérifiant la connectivité du serveur de base de données ou en installant les outils clients de base de données 32 bits associés (comme les clients SQL ou Oracle) sur l'ordinateur.

Affichage manquant de la fenêtre d'invite dans l'explorateur DSM en connexion en mode réunion

Symptôme :

Lorsque j'ouvre l'explorateur DSM dans un gestionnaire de domaines, que je clique droit sur l'agent et établis une connexion en mode réunion, l'application n'affiche pas la fenêtre d'invite.

Solution :

Vérifiez que le package libatk-1.0.so.0 est installé sur l'agent.

Problèmes lors de la modification de la configuration du serveur de démarrage du mode tftp en mode Accès partagé dans une installation de cluster

Symptôme :

Lorsque vous modifiez la configuration du serveur de démarrage du mode tftp en mode Accès partagé dans une installation de cluster, l'erreur suivante est renvoyée :

ERROR: trying to create camenu share (Erreur lors de la création du partage camenu)
ERROR: trying to create sxpsetup share (Erreur lors de la création du partage sxpsetup)

Solution :

Pour définir le mode Accès partagé comme configuration du serveur de démarrage sans obtenir aucune erreur dans le cluster d'applications de Client Automation, configurez un serveur de modularité distant.

Problème relatif à la taille des composants ITCM et CIC dans le menu Ajout/Suppression de programmes

Symptôme :

Après l'installation de Client Automation Version 12.9 ou une mise à niveau, la taille de Client Automation, du client d'importation de contenu (CIC), du gestionnaire de patchs et des autres composants Client Automation ne s'affiche pas sous Panneau de configuration, Ajout/Suppression de programmes.

Solution :

L'obtention de la taille et son affichage sous Panneau de configuration, Ajout/Suppression de programmes est une propriété de Windows et non d'InstallShield. Ce comportement est dû à une modification de la fonctionnalité utilisée par Microsoft pour calculer la taille approximative sur Windows. La taille de chaque composant installé est estimée à l'aide de l'algorithme du système d'exploitation. Cet algorithme peut varier selon les versions de Windows, ce qui affecte l'affichage de ces données.

Pour afficher les estimations de taille, procédez comme suit :

Procédez comme suit:

Microsoft utilise exclusivement la clé de registre *EstimatedSize* pour calculer l'estimation de taille sous Ajout/Suppression de programmes. Pour remplir les estimations de taille, vous pouvez modifier manuellement la clé de registre *EstimatedSize* dans HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{PRODUCT_CODE}. Pour plus d'informations, consultez la documentation Microsoft.

Erreur et retard lors de la connexion au site de support technique

Symptôme :

Lorsque vous tentez d'accéder à la page de support technique à partir des fenêtres A propos de de Client Automation, une erreur de script s'affiche après un délai.

Solution :

Appuyez sur Oui et la page de support technique s'affiche après un instant. Notez que ce retard est spécifique à Internet Explorer 7 uniquement.

Prise en charge de SELinux pour les composants de Client Automation

Les systèmes Linux pour lesquels le système de sécurité SELinux est activé, requièrent des paramètres SELinux spécifiques pour les composants de Client Automation suivants :

Services Web et console Web de DSM

L'installation des services Web et de la console Web de Client Automation est effectuée sans erreur sur les systèmes pour lesquels SELinux est défini sur le mode strict. Toutefois, pour travailler avec ces composants, basculez sur le mode **permissif** de la manière suivante :

Procédez comme suit:

- Ouvrez le fichier /etc/selinux/config dans un éditeur de texte.
- Remplacez l'indicateur SELINUX=enforcing par SELINUX=**permissive.**
- Réinitialisez le système.

Affichage de texte indésirable dans l'interface utilisateur du programme d'installation en japonais

Applicable aux versions japonaises de Linux.

Symptôme :

Lorsque vous lancez le programme d'installation en japonais sur Linux, du texte indésirable est affiché sur l'interface utilisateur.

Solution :

Lancez le programme d'installation du produit en mode de ligne de commande ou utilisez l'installation silencieuse à l'aide du fichier de réponse.

Problème avec les chaînes à l'invite de commande

Valide sur Windows et Linux

Symptôme :

Lorsque vous exécutez des commandes dans un environnement localisé, des problèmes surviennent avec les chaînes à l'invite de commande.

Solution :

Pour corriger ce problème, effectuez les changements suivants :

Sous Windows :

Ce problème se produit lorsque la page de codes par défaut de l'environnement n'est pas prise en charge.

Par exemple, lorsque la page de codes par défaut pour l'allemand et le français est 850, les chaînes d'invite de commande s'affichent de manière irrégulière. Notez que pour l'allemand et le français, Client Automation prend en charge la *page de codes 1252.* Vous pouvez réinitialiser la page de codes aux paramètres de l'environnement en exécutant la commande suivante :

```
chcp  1252
```

Sour Linux :

Vous pouvez réinitialiser le paramètre Langue de la façon suivante :

1. Accédez au dossier *cd\etc\sysconfig*, puis ouvrez le fichier *i18n.*
2. Modifiez le paramètre Lang de la façon suivante :

   Exemple :
   (Pour l'allemand) Lang=de_DE.UTF-8

   (Pour le français) Lang=fr_FR.UTF-8

Erreur lors du chargement des bibliothèques partagées sur un nouveau système d'exploitation Linux 64 bits

Symptôme :

Plusieurs fonctionnalités de DSM (comme cfSysTray, la connexion de contrôle à distance, les propriétés dsm) ne fonctionnent pas sur les nouveaux systèmes d'exploitation Linux 64 bits. Par exemple, lorsque vous exécutez cfSystray, le message d'erreur suivant s'affiche :

[root@hostname]# cfsysTray show
cfSysTray: error while loading shared libraries: libgtk-x11-2.0.so.0: wrong ELF class: ELFCLASS64.

Solution :

DSM est une application 32 bits et requiert des versions 32 bits des bibliothèques du système d'exploitation. Les commandes DSM échouent, car le système d'exploitation Linux 64 bits n'inclut aucune bibliothèque de système d'exploitation 32 bits. Par défaut, ces bibliothèques ne sont pas installées sur les nouveaux systèmes d'exploitation Linux 64 bits.

Pour installer les bibliothèques requises, consultez le site du support de CA ou contactez votre administrateur système.

Echec de l'installation d'agent sur Solaris avec une erreur

Symptôme :

Echec de l'installation d'agent sur Solaris 10 avec l'erreur suivante dans le fichier journal :

ld.so.1: setup: fatal: libCstd.so.1: version `SUNW_1.4.2' not found (required by file /opt/CA/DSM/capki/setup)
ld.so.1: setup: fatal: libCstd.so.1: open failed: No such file or directory Killed /opt/CA/DSM/capki/setup install caller=CAITCM verbose env=all failed with return code = 137
11:43:58 !! Script executed with error: 137
Script or command "capki/pkiInst" failed with exit code 137.
Reason:The script or command encountered a problem.
Action: Find further details in the installation log file /opt/CA/SharedComponents/installer/log/ca-dsm.log.

Solution :

L'installation d'agent sur Solaris 10 échoue, car la version de la bibliothèque libCstd est incompatible. Pour résoudre ce problème, installez le patch de système d'exploitation Solaris 119964-12 ou une version ultérieure.

Remote Control sur Windows 8 et 8.1 en mode sécurisé

Symptôme :

Remote Control sur Windows 8, Windows 8.1, Windows Server 2012 et Windows Server 2012 R2 prend en charge tous les modes de connexion sauf le mode de contrôle sécurisé.

Solution :

Une solution est en cours de développement et sera mise à votre disposition dans la prochaine version majeure.

Connexion à la MDB impossible

Symptôme :

Lorsque vous installez CIC, le programme d'installation s'arrête avec le message d'erreur suivant :

Impossible d'établir la connexion à la MDB. Vérifiez les informations d'identification du serveur de MDB.

Solution :

Vérifiez que les informations d'identification de MDB respectent les stratégies de mot de passe. CIC prend en charge les caractères alphanumériques et les caractères spéciaux suivants dans les mots de passe de MDB :

SQL

~ ! # $ * ( ) _ + - { } [ ] ? / @

Oracle

$ _

- Réinitialisez le mot de passe de MDB pour que le programme d'installation s'exécute normalement.

Pour plus d'informations sur la stratégie de mot de passe de base de données MS SQL et Oracle, visitez les sites Web des sociétés respectives.

Echec de démarrage du gestionnaire DSM après la mise à niveau de CAM

Lors de l'installation de Client Automation, CA Message Queuing (CAM) est généralement mis à niveau simultanément. Si le démarrage du gestionnaire DSM échoue en raison d'une impossibilité de connexion à CAM, arrêtez la version de CAM actuellement exécutée ou redémarrez-la après l'installation de Client Automation.

Suppression des journaux du dossier temporaire

Symptôme :

Lorsque j'installe Client Automation sur l'ordinateur sur lequel les services Bureau à distance sont configurés, les journaux dans le dossier temporaire sont supprimés après la déconnexion de l'utilisateur ou lors du redémarrage de l'ordinateur.

Solution :

Procédez de la manière suivante :

- Accédez à *Services Bureau à distance, Hôte de session Bureau à distance, Ne pas supprimer le dossier temporaire à la sortie*.
    - Si le statut est défini sur Activé, les dossiers temporaires par session de l'utilisateur seront conservés lorsqu'il se déconnectera d'une session.
    - Si le statut est défini sur Désactivé, les dossiers temporaires seront supprimés lorsqu'un utilisateur se déconnecte, même si l'administrateur spécifie le contraire dans l'outil de configuration de l'hôte de session Bureau à distance.
    - Si le statut est défini sur Non configuré, les services Bureau à distance supprimeront les dossiers temporaires de l'ordinateur distant lors de la déconnexion, sauf en cas d'indication contraire par l'administrateur de serveur.

Remarque : Le chemin d'accès aux services Bureau à distance varie selon la version du système d'exploitation.

Blocage du programme d'installation de la MDB en cas de définition incorrecte de la variable ORACLE_HOME ou du mot de passe ca_itrm

Si la variable d'environnement ORACLE_HOME est définie incorrectement, le programme d'installation de la MDB se bloquera lors d'une installation autonome, de la réinstallation, ou de la mise à niveau. Définissez la variable ORACLE_HOME correctement ou supprimez la valeur dans cette variable d'environnement. La valeur pour ORACLE_HOME est alors récupérée à partir du fichier de réponse.

Si vous avez saisi un mot de passe ca_itrm incorrect lors d'une réinstallation ou de la mise à niveau (interactive ou autonome), le programme d'installation de la MDB se bloquera. Vérifiez que le mot de passe de ca_itrm est correctement saisi.

Erreur d'installation due à une instance nommée et l'ID de port

Une erreur d'installation peut se produire sur Microsoft SQL Server en raison des propriétés de l'instance nommée et de l'ID de port. Vérifiez que l'ID de port spécifié est correct.

Entrées inutilisées dans le fichier de réponse

Le fichier de réponse généré et le modèle install.rsp contiennent les entrées de Microsoft SQL suivantes : ITRM_DBSQLPORT=1433 et ITRM_SQLADMINUSER=sa. Ces entrées sont inutilisées et ignorées par le programme d'installation de la MDB.

Erreur de synchronisation à partir de la MDB SQL vers la cible de la MDB Oracle

Symptôme :

Lorsque j'effectue la synchronisation à partir d'une source contenant la MDB sur SQL Server vers une cible contenant la MDB sur Oracle 11g, l'erreur suivante apparaît dans les journaux du moteur pour ITCM R12.5 SP1 :

RecImpl_Ado |RecImpl_Ado.cpp |001371|ERROR | FieldLng encounters an undefined VT type =5 for 14

RecImpl_Ado |RecImpl_Ado.cpp |001373|ERROR | FieldLng encounters an undefined VT type =0

Solution :

Appliquez le correctif test RO43621. Suivez les instructions du fichier Readme du correctif test.

Erreur de synchronisation sur une MDB cible sous Oracle

Symptôme :

Lorsque j'effectue la synchronisation avec une cible MDB sous Oracle, le message d'erreur suivant apparaît dans le fichier journal du moteur :

```
ERROR  | ERROR:OCIStmtExecute() failed
```

Solution :

Appliquez le correctif test RO43619. Suivez les instructions du fichier Readme du correctif test.

Pour résoudre ce problème, appliquez le patch RO43619. Pour plus d'informations sur la procédure à suivre pour appliquer ce patch, consultez la documentation de la solution RO43619 sur le site du support de CA.

Echec de la connexion unifiée à partir de la console Web sur la Console d'administration Web (WAC) autonome

Symptôme :

Lorsque j'accède à la fonctionnalité de connexion unifiée de la console Web à partir d'un navigateur pris en charge sous Windows 2008 et versions ultérieures, la connexion échoue et m'invite à effectuer une connexion explicite.

Solution :

Procédez comme suit :

1. Vérifiez que le contrôleur de domaine est placé sous Windows 2008 ou versions ultérieures avec le paramètre de stratégie local suivant :
   - Accès réseau : modèle de partage et de sécurité pour les comptes locaux : Classic
   - Accès réseau : niveau d'authentification du gestionnaire de réseau local : Envoyer des réponses LM et NTLM
   - Sécurité réseau : vérifiez que la sécurité de session minimum pour des clients NTLM SSP (y compris RPC sécurisé) est définie sur No minimum.
2. Vérifiez que le gestionnaire de domaines est placé sous Windows 2008 ou versions ultérieures et définissez la stratégie locale comme indiqué à l'étape 1.
3. Vérifiez que le registre du gestionnaire de domaines est placé sous Windows 2008 ou versions ultérieures et désactivez la case à cocher de bouclage :
   Procédez comme suit :
   a. Cliquez sur Démarrer, Exécuter.
   b. Saisissez Regedit. Cliquez sur OK.
   c. Dans l'éditeur de registre, recherchez la clé de registre suivante et cliquez dessus :
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
   d. Cliquez avec le bouton droit de la souris sur LSA et pointez sur Créer. Cliquez sur la valeur DWORD.
   e. Saisisset DisableLoopbackCheck. Appuyez sur ENTREE.
   f. Cliquez avec le bouton droit de la souris sur DisableLoopbackCheck. Cliquez sur Modifier.
   g. Dans la zone de données de valeur, saisissez 1. Cliquez sur OK.
4. Dans la zone Utilisateur, vérifiez les paramètr.es du navigateur (Internet Explorer ou Firefox).

   Remarque : Pour plus d'informations sur les paramètres du navigateur pour la connexion unifiée, consultez la rubrique Configuration des paramètres du navigateur pour la connexion unifiée dans l'*Aide de la console Web*.

5. Si le navigateur est sur l'ordinateur de classes de serveur, utilisez les paramètres de stratégie locaux indiqués à l'étape 1.

Utilisation élevée de l'UC après la mise à niveau du gestionnaire DSM

Symptôme :

Après avoir mis à niveau le gestionnaire DSM vers la version actuelle, l'utilisation de l'UC est élevée à cause d'anciens modules de cryptage exécutés via Tomcat 7 et JRE 1.7.

Solution :

Ce problème survient lorsque vous mettez à niveau le gestionnaire DSM de CA ITCM, sans inclure Patch Manager dans la mise à niveau. Mettez à niveau Patch Manager vers la version de CA ITCM actuelle.

Echec du déploiement de l'infrastructure en cas d'implication d'une machine virtuelle Windows 2012

Symptôme :

Le déploiement de l'infrastructure échoue si l'un des composants suivants est une machine virtuelle Windows 2012.

- Gestionnaire de domaines
- Serveur de modularité.
- Ordinateur cible

Solution :

Appliquez les informations de l'article de base de connaissances VMware suivant : Possible data corruption after a Windows 2012 virtual machine network transfer (2058692).

Impossible de collecter l'inventaire matériel à l'aide du client Windows 32 bits pour Oracle 12.1.0.1

Symptôme :

Lorsque CA Client Automation est installé avec une MDB sur le serveur Oracle 12c et que le client Windows 32 bits pour Oracle 12.1.0.1 est utilisé pour se connecter à la base de données, le matériel n'est pas collecté sur le gestionnaire de domaines ou le gestionnaire d'entreprise répliqué.

Solution :

Ce problème survient lorsque le fichier oraodm12.dll n'est pas disponible à l'emplacement du client Oracle.

Procédez comme suit:

1. Téléchargez le fichier oraodm12.dll à partir du site de support d'Oracle.
2. Copiez le fichier à l'emplacement suivant :

   <emplacement_client_Oracle_12.1>\bin\

Pour plus d'informations, consultez le document 1593348.1 sur le site du support d'Oracle.

Annexe A: Fichier de configuration du service d'automatisation

Le fichier de configuration du service d'automatisation contient des paramètres de configuration que la migration automatisée utilise pour diverses tâches. Bien que tous les paramètres soient décrits dans cette section, certains sont uniquement fournis à titre informatif. Il est recommandé de ne pas changer les paramètres qui sont uniquement informatifs.

Remarque : Un nombre entier dans le fichier automation.config ne doit pas contenir ni être entouré par des espaces. Lorsque vous spécifiez un nombre entier dans le fichier automation.config, vérifiez l'absence de tout espace dans la valeur et autour de cette dernière. Tout espace dans le nombre entier peut entraîner un dysfonctionnement du service d'automatisation.

AssessmentServiceEPR

Définit l'URL de point de terminaison du service d'évaluation. Ce paramètre est uniquement fourni à titre informatif.

ITCMEPR

Définit l'URL de terminal du service Web de CA ITCM. Ce paramètre est uniquement fourni à titre informatif.

ITPAMEPR

Définit l'URL de point de terminaison du service Web de CA IT PAM. Ce paramètre est uniquement fourni à titre informatif.

AutomationServiceEPR

Définit l'URL de point de terminaison du service d'automatisation. Ce paramètre est uniquement fourni à titre informatif.

JNI_BIN_PATH

Définit le chemin d'accès JNI pour obtenir les valeurs comstore. Ce paramètre est uniquement fourni à titre informatif.

DEFAULT_MANAGER

Définit le nom du gestionnaire par défaut de la console Web et des services Web de CA ITCM. Ce paramètre est uniquement fourni à titre informatif.

WipeAndReloadProcess

Définit le chemin d'accès à la définition de processus de CA IT PAM pour la migration de type réinitialisation et rechargement. Changez ce paramètre uniquement si vous avez personnalisé la définition de processus.

MachineReplacementProcess

Définit le chemin d'accès à la définition de processus de CA IT PAM pour la migration de type remplacement d'ordinateur. Changez ce paramètre uniquement si vous avez personnalisé la définition de processus.

MaxNumberOfITPAMInstances

Définit le nombre maximum d'instances CA IT PAM que le service d'automatisation peut exécuter simultanément. Changez cette valeur en fonction de la charge que votre serveur CA IT PAM peut gérer.

Remarque : Le service d'automatisation crée une seule instance CA IT PAM par ordinateur dans le job de migration.

ProcessLaunchInterval

Définit l'intervalle (en secondes) entre la création d'instances CA IT PAM.

TimeOutForOSIMJobs

Définit le délai d'expiration (en secondes) avant lequel l'ordinateur doit commencer le job OSIM. Une fois le délai d'expiration écoulé, les jobs OSIM sont annulés et le job de migration de système d'exploitation échoue pour l'ordinateur.

WaitForBootServer

Indique que l'activation de l'installation de système d'exploitation attend qu'un serveur de démarrage sélectionne la cible et contacte le gestionnaire de domaines.

WaitForOSImage

Indique que l'activation de l'installation de système d'exploitation attend que l'image de système d'exploitation et de démarrage requise soit disponible sur le serveur de démarrage affecté.

WakeOnLAN

Indique si le serveur de démarrage doit sortir de veille l'ordinateur cible avant l'installation du système d'exploitation.

Reboot

Indique si le serveur de démarrage doit imposer le redémarrage à l'ordinateur cible avant d'activer l'installation (si défini sur true).

ContainerPriority

Définit la priorité pour des conteneurs de jobs logiciels créés pour le job de migration.

DeliveryCalender

Définit le nom du calendrier de livraison que vous voulez utiliser. Laissez ce paramètre vide si vous ne souhaitez pas utiliser un calendrier de livraison.

IgnoreJobCalendarsOnTargetComputers

Spécifie si l'option de job "Ignorer les calendriers de jobs sur les ordinateurs cibles" doit être définie lors de la création d'un conteneur RAC. Si cette stratégie est définie sur False, les calendriers ne sont pas ignorés sur les ordinateurs cibles. Si elle est définie sur True, les calendriers sont ignorés sur les ordinateurs cibles.

JobsTriggerSS

Indique que le serveur de modularité doit initialiser et exécuter le job à l'heure planifiée.

RemoveInstallationHistory

Indique que les enregistrements d'installation existants doivent être supprimés avant d'activer le processus d'installation, afin d'éviter que le job échoue avec l'état Déjà installé.

RunFromSS

Indique si le programme de vérification des jobs de l'ordinateur cible doit cesser de communiquer avec le serveur au cours de l'exécution du job. Une fois le job terminé, l'agent se reconnecte au serveur pour signaler l'état du job.

TimesRelativeToEM

Indique que l'heure d'activation spécifiée doit être interprétée en tant qu'heure universelle. Le décalage horaire configuré sur chaque gestionnaire de domaines est pris en compte pour convertir l'heure communiquée en fonction de l'heure système locale.

UseDeliveryCalender

Indique si le calendrier de livraison doit être utilisé pour le job.

SoftwareBlackList

Définit la liste de packages logiciels utilisés pour exclure des ordinateurs du job de migration de système d'exploitation. Les ordinateurs sur lesquels un de ces packages logiciels est installé sont automatiquement exclus de la migration de système d'exploitation.

MaximumDelayOfJobContainer

Définit le délai pendant lequel le conteneur de jobs attend des ordinateurs supplémentaires après l'ajout du premier ordinateur, avant de se sceller. Des conteneurs supplémentaires sont automatiquement créés, si nécessaire.

MaxNumberOfTargetsPerJobContainer

Définit le nombre maximum d'ordinateurs cibles par conteneur de jobs. Une fois que le conteneur de jobs a atteint cette limite, il se ferme et un nouveau conteneur de jobs est créé pour les ordinateurs restants.

LastTargetInContainerOptimization

Indique si le conteneur de jobs doit être activé immédiatement lorsqu'il ne reste plus aucune cible dans le job de migration. Le conteneur est activé immédiatement même si les cibles dans le conteneur sont moins nombreuses que la valeur spécifiée par le paramètre MaxNumberOfTargetsPerJobContainer et sans attendre que le délai MaximumDelayOfJobContainer soit écoulé. Ce paramètre est uniquement fourni à titre informatif.

Valeur par défaut : True

RenamePackageName

Définit le package logiciel utilisé pour renommer les ordinateurs. Ce paramètre est uniquement fourni à titre informatif.

RenamePackageVersion

Définit la version du package logiciel utilisé pour renommer les ordinateurs. Ce paramètre est uniquement fourni à titre informatif.

RenameProcedure

Définit la procédure de package logiciel utilisée pour renommer les ordinateurs. Ce paramètre est uniquement fourni à titre informatif.

AutomationJobScheduleInterval

Définit le délai (en secondes) pendant lequel le service d'automatisation attend avant de planifier le job d'automatisation suivant.

AutomationJobSchedulerBatchSize

Définit le nombre de cibles planifiées par le service d'automatisation avant de vérifier le statut d'instance ITPAM des cibles planifiées et met à jour le statut en le définissant sur Migration réussie ou Echec de la migration. Vous pouvez changer cette valeur en fonction de la charge sur le serveur CA IT PAM et de la fréquence de mise à jour souhaitée pour le statut de la cible.

Propriétés Log4j

Définit les propriétés log4j suivantes :

– log4j.rootLogger

– log4j.appender.A1

– log4j.appender.A1.layout

– log4j.appender.A1.layout.ConversionPattern

– log4j.appender.A1.MaxFileSize

– log4j.appender.A1.MaxBackupIndex

Par exemple, vous pouvez changer les paramètres suivants pour modifier le niveau de journalisation, la taille de fichier ou le nombre de fichiers journaux créés :

log4j.rootLogger=ERROR, A1

Remarque : Remplacez cette valeur par DEBUG ou INFO pour changer le niveau de journalisation en conséquence.

log4j.appender.A1.MaxFileSize=5000KB

log4j.appender.A1.MaxBackupIndex=1

Remarque : Pour plus d'informations sur les propriétés Log4j, reportez-vous à la documentation de org.apache.log4j.PropertyConfigurator.

Annexe B: Ports utilisés par CA Client Automation

Les tableaux ci-après décrivent en détail l'utilisation des ports des différents composants DSM. Ces tableaux sont exhaustifs et se recoupent afin de fournir une vue complète pour chaque composant.

Ce chapitre traite des sujets suivants :

Observations générales sur l'utilisation de port

En général, pour la majorité des communications entre les composants sur le réseau, Client Automation nécessite l'ouverture de deux ports uniquement, plus précisément le port 4104 UDP pour le trafic (généralement léger) des messages et le port 4728 TCP pour le trafic (généralement de masse) de flux.

Par défaut, les communications distantes à l'aide de CA Message Queuing (CAM) utilisent le protocole UDP via le port 4104, comme indiqué dans les tableaux ci-après. Vous pouvez configurer CAM pour utiliser TCP pour les communications distantes (ce qui peut être préférable dans certaines circonstances). Le cas échéant, le protocole TCP est utilisé avec un port source ANY et un port d'écoute dont le numéro est 4105. Si SSA est installé sur l'ordinateur local, les communications via le port TCP de CAM sont mises en multiplexage via le port 7163 de SSA pour toutes les connexions de sortie par défaut. Les communications distantes par le biais de CAM via TCP ne sont pas documentées dans les tableaux. CAM est aussi largement utilisé pour les communications locales, c'est à dire entre des composants fonctionnant sur le même ordinateur. Dans ce cas, c'est le port TCP 4105 qui est utilisé.

Certaines fonctions présentes dans Client Automation peuvent recourir au partage des fichiers si la configuration le prévoit. Dans ce cas, les ports de partage de fichier appropriés doivent être ouverts. Les numéros de port spécifiques varient en fonction de l'environnement d'exploitation (plate-forme) et des mécanismes disponibles et configurés.

Les ports de partage de fichiers types sont les suivants :

Windows

Soit 139/TCP (ancien style), soit 445/TCP (nouveau style)

Linux et UNIX

2049/TCP (NFS)

Ports utilisés par le gestionnaire d'entreprise

Les tableaux suivants offrent un aperçu des ports utilisés pour les communications depuis et vers le gestionnaire d'entreprise.

Communications depuis le gestionnaire d'entreprise

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire d'entreprise	Non spécifiée	Gestionnaire d'entreprise	4105	TCP	Tous	Communications locales via CAM

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire d'entreprise	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Gestionnaire d'entreprise	Non spécifiée	Serveur de répertoires	389	TCP	Tous	Accès au répertoire LDAP
Gestionnaire d'entreprise	Non spécifiée	Serveur de répertoires	636	TCP	Tous	accès au répertoire LDAP via SSL
Gestionnaire d'entreprise	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers DTS

Communications vers le gestionnaire d'entreprise

De	Port	A	Port	Protocole	Produit	Description
Explorateur	4104	Gestionnaire d'entreprise	4104	UDP	Tous	Communications via CAM sur le réseau
Navigateur Web	Non spécifiée	Gestionnaire d'entreprise	80	Serveurs	Tous	Accès à la console Web
Client des services Web	Non spécifiée	Gestionnaire d'entreprise	80	Serveurs	Tous	Accès à l'API des services Web depuis une application cliente distante
Gestionnaire de domaines	Non spécifiée	Gestionnaire d'entreprise	4728	TCP	Software Delivery	Transfert de fichiers DTS
Explorateur	Ports de partage de fichiers	Gestionnaire d'entreprise	Ports de partage de fichiers	UDP	Software Delivery	Transfert de fichiers basé sur serveur NOS
Explorateur	Non spécifiée	Gestionnaire d'entreprise	4728	TCP	Software Delivery	Transfert de fichiers non-NOS
Outil de packaging	4104	Gestionnaire d'entreprise	4104	UDP	Software Delivery	Communications via CAM sur le réseau

Remarques :

- Si les communications HTTP sécurisées sont configurées pour être utilisées par la console Web et les composants des services Web, le port 443 (par défaut) est utilisé pour écouter le gestionnaire de domaine ou d'entreprise.
- La console Web utilise Apache Tomcat. Par défaut, Tomcat est installé et configuré pour utiliser les ports 8090 (démarrage), 8095 (arrêt), et 8020 (ajp13). Généralement, ces derniers sont cependant utilisés en local uniquement.

Ports utilisés par le gestionnaire de domaines

Les tableaux suivants offrent un aperçu des ports utilisés pour les communications entre les gestionnaires de domaine.

Communications du gestionnaire de domaine

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire de domaines	Non spécifiée	Gestionnaire de domaines	4105	TCP	Tous	Communications locales via CAM
Gestionnaire de domaines	4104	Gestionnaire d'entreprise	4104	UDP	Tous	Communications via CAM sur le réseau
Gestionnaire de domaines	4104	Moteur de domaine distant	4104	UDP	Tous	Communications via CAM sur le réseau
Gestionnaire de domaines	4104	Serveur de modularité	4104	UDP	Tous	Communications via CAM sur le réseau
Gestionnaire de domaines	Non spécifiée	Serveur de répertoires	389	TCP	Tous	Accès au répertoire LDAP
Gestionnaire de domaines	Non spécifiée	Serveur de répertoires	636	TCP	Tous	accès au répertoire LDAP via SSL
Gestionnaire de domaines	4104	Explorateur	4104	UDP	Tous	Communications via CAM sur le réseau
Gestionnaire de domaines	Non spécifiée	Gestionnaire d'entreprise	4728	TCP	Software Delivery	Transfert de fichiers DTS : accusés de réception de commande de distribution
Gestionnaire de domaines	Non spécifiée	Serveur de modularité	4728	TCP	Software Delivery	Transfert de fichiers DTS : transfert de package

Communications vers le gestionnaire de domaines

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire d'entreprise	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Explorateur	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Serveur de modularité	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Navigateur Web	Non spécifiée	Gestionnaire de domaines	80	Serveurs	Tous	Accès à la console Web
Client des services Web	Non spécifiée	Gestionnaire de domaines	80	Serveurs	Tous	Accès à l'API des services Web depuis une application cliente distante
Moteur de domaine distant	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Agent	4104	Gestionnaire de domaines	4104	UDP	Remote Control Software Delivery	Communications via CAM sur le réseau Catalogue SD, Auth. Hôte RC, Visionneuse RC GAB
Serveur de modularité	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : fichiers de sortie de job
Gestionnaire d'entreprise	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers DTS : transfert de package
Explorateur	Ports de partage de fichiers	Gestionnaire de domaines	Ports de partage de fichiers	TCP/UDP	Software Delivery	Transfert de fichiers basé sur serveur NOS : enregistrement du package
Explorateur	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : enregistrement du package
Outil de packaging	4104	Gestionnaire de domaines	4104	UDP	Software Delivery	Données de contrôle d'enregistrement de package

De	Port	A	Port	Protocole	Produit	Description
Outil de packaging	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : enregistrement du package

Remarques :

- Si les communications HTTP sécurisées sont configurées pour être utilisées par la console Web et les composants des services Web, le port 443 (par défaut) est utilisé pour écouter le gestionnaire de domaine ou d'entreprise.
- La console Web utilise Apache Tomcat. Par défaut, Tomcat est installé et configuré pour utiliser les ports 8090 (démarrage), 8095 (arrêt), et 8020 (ajp13). Généralement, ces derniers sont cependant utilisés en local uniquement.

Ports utilisés par le déploiement de l'infrastructure

Le déploiement de l'infrastructure fait partie du gestionnaire de domaine. L'utilisation des ports par le déploiement de l'infrastructure est présentée dans une section distincte afin de souligner le fait que les ports concernés doivent être ouverts uniquement pendant que le déploiement de l'infrastructure est utilisé.

Les ports mentionnés dans les tableaux ci-après (à l'exception du port 7) sont utilisés pour répercuter le logiciel d'injection du déploiement de l'infrastructure depuis le gestionnaire de domaine. Si un client souhaite installer le logiciel d'injection manuellement ou ne veut pas utiliser du tout infrastructure deployment, il n'est pas obligé d'ouvrir ces ports. Il n'est pas nécessaire d'ouvrir tous les ports pour toutes les cibles. Les ports n'ont pas besoin de rester ouverts ; ils doivent uniquement être ouverts pendant la période de déploiement.

En outre, le client peut ouvrir un sous-ensemble de ports MS Share/Telnet et FTP/SSH, selon les mécanismes de communication utilisés.

Communications du gestionnaire de domaine

De	Port	A	Port	Protocole	Produit	Description

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire de domaines	Non spécifié(e)	Cible	7	TCP	Tous	Demande d'écho, utilisée pendant l'analyse de cible. Vous pouvez désactiver l'utilisation de ce port à l'aide du paramètre approprié dans la politique de configuration.
Gestionnaire de domaines	Ports de partage de fichiers	Cible	Ports de partage de fichiers	TCP UDP	Tous	Transfert des fichiers du package de logiciel d'injection basé sur le protocole Windows NOS. Utilisation d'ADMIN$
Gestionnaire de domaines	Non spécifié(e)	Cible	135	TCP	Tous	Appel RPC Windows pour commencer l'installation du logiciel d'injection
Gestionnaire de domaines	Non spécifié(e)	Cible	21	TCP	Tous	Transfert des fichiers du package de logiciel d'injection basé sur le protocole FTP.
Gestionnaire de domaines	Non spécifié(e)	Cible	22	TCP	Tous	Transfert des fichiers du package de logiciel d'injection basé sur le protocole UNIX ssh/SFTP. Communications effectuées à partir du gestionnaire de domaines
Gestionnaire de domaines	Non spécifié(e)	Cible	23	TCP	Tous	Connexion Telnet UNIX utilisée pour lancer le transfert des fichiers du package de logiciel d'injection basé sur le protocole FTP sur la cible.
Gestionnaire de domaines	Non spécifié(e)	Cible	4104	UDP	Tous	Méthode de communication préférée de CAM
Gestionnaire de domaines	Non spécifié(e)	Cible	4105 7163	TCP	Tous	Méthode de communication préférée de CAM Le port 7163 est utilisé par SSA pour le multiplexage de ports.

Communications vers le gestionnaire de domaines

De	Port	A	Port	Protocole	Produit	Description
Cible	Non spécifié(e)	Gestionnaire de domaines	20 21	TCP	Tous	Transfert des fichiers du package de logiciel d'injection basé sur le protocole FTP.
Cible	Non spécifié(e)	Gestionnaire de domaines	4104	UDP	Tous	Méthode de communication préférée de CAM
Cible	Non spécifié(e)	Gestionnaire de domaines	4105 7163	TCP	Tous	Méthode de communication préférée de CAM Le port 7163 est utilisé par SSA pour le multiplexage de ports.

Ports utilisés par le serveur de modularité

Les tableaux suivants offrent un aperçu des ports utilisés pour les communications entre les serveurs de modularité.

Communications depuis le serveur de modularité :

De	**Port**	**A**	**Port**	**Protocole**	**Produit**	**Description**
Serveur de modularité	Non spécifiée	Serveur de modularité	4105	TCP	Tous	Communications locales via CAM
Serveur de modularité	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Serveur de modularité	4104	Moteur de domaine	4104	UDP	Tous	Communications via CAM sur le réseau
Serveur de modularité	4104	Agent	4104	UDP	Tous	Communications via CAM sur le réseau Configuration, Vérification des jobs déclencheur SD Vérification des jobs déclencheur AM

De	Port	A	Port	Protocole	Produit	Description
Serveur de modularité	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : Fichiers de sortie de job
Serveur de modularité	Non spécifiée	Agent	4728	TCP	Software Delivery	Transfert de fichiers DTS : Transfert de package
Serveur de modularité	554	Agent	554	TCP	Software Delivery	RTSP (non sécurisé) pour des services d'application virtualisée App-V
Serveur de modularité	322	Agent	322	TCP	Software Delivery	RTSPS (sécurisé) pour des services d'application virtualisée App-V

Communications vers le serveur de modularité

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire de domaines	4104	Serveur de modularité	4104	UDP	Tous	Communications via CAM sur le réseau
Moteur de domaine	4104	Serveur de modularité	4104	UDP	Tous	Communications via CAM sur le réseau
Agent	4104	Serveur de modularité	4104	UDP	Tous	Communications via CAM sur le réseau
Agent	Non spécifiée	Serveur de modularité	4728	TCP	Tous	Transfert de fichiers non-NOS Transfert de données de sauvegarde
Agent	Ports de partage de fichiers	Serveur de modularité	Ports de partage de fichiers	TCP	Software Delivery	Transfert de fichiers basé sur serveur NOS
Gestionnaire de domaines	Non spécifiée	Serveur de modularité	4728	TCP	Software Delivery	Transfert de fichiers DTS : Transfert de package
Agent	554	Serveur de modularité	554	TCP	Software Delivery	RTSP (non sécurisé) pour des services d'application virtualisée App-V
Agent	322	Serveur de modularité	322	TCP	Software Delivery	RTSPS (sécurisé) pour des services d'application virtualisée App-V

Ports utilisés par le serveur amorçable

Le serveur de démarrage fait partie du serveur de modularité. L'utilisation de ses ports est présentée dans une section distincte afin de souligner le fait que les ports concernés doivent être ouverts uniquement si les fonctions de gestion d'installation du SE (OSIM) sont utilisées.

Communications vers le serveur de modularité

De	Port	A	Port	Protocole	Produit	Description
Cible	68	Serveur de modularité	67	UDP	Software Delivery	Client de protocole d'amorce – bootpc
Cible	Non spécifiée	Serveur de modularité	69	UDP	Software Delivery	Transfert de fichiers trivial (TFTP)
Cible PXE	Non spécifiée	Serveur de modularité	4011	UDP	Software Delivery	(facultatif) Autre service d'amorçage – altserviceboot.binl (PXE) Si le port 4011 n'est pas disponible, le port 67 est utilisé à la place.
Cible	Ports de partage de fichiers	Serveur de modularité	Ports de partage de fichiers	TCP/UDP	Software Delivery	Transfert de fichiers basé sur serveur NOS

Ports utilisés par le moteur

Les tableaux suivants offrent un aperçu des ports utilisés pour les communications vers et depuis un moteur.

Communications depuis le moteur

De	Port	A	Port	Protocole	Produit	Description
N'importe quel moteur	Non spécifiée	N'importe quel moteur	4105	TCP	Tous	Communications locales via CAM
N'importe quel moteur	Non spécifiée	Serveur de contenu	443 ou 5250	TCP	Tous	Téléchargement de signature logicielle depuis le site Web CA Content

De	Port	A	Port	Protocole	Produit	Description
N'importe quel moteur	Non spécifiée	Serveur de répertoires	389	TCP	Tous	Accès au répertoire LDAP : Synchronisation de répertoires, Requêtes, Rapports
N'importe quel moteur	Non spécifiée	Serveur de répertoires	636	TCP	Tous	Accès au répertoire LDAP via SSL : Synchronisation de répertoires, Requêtes, Rapports
N'importe quel moteur	Non spécifiée	Serveur SMTP	25	TCP/UDP	Gestion des actifs	Envoi de courriel en cas de violation de stratégie
Moteur de domaine	4104	Serveur de modularité	4104	UDP	Tous	Communications via CAM sur le réseau
Moteur de domaine distant	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Moteur d'entreprise distant	4104	Gestionnaire d'entreprise	4104	UDP	Tous	Communications via CAM sur le réseau

Communications vers le moteur

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire d'entreprise	4104	Moteur d'entreprise distant	4104	UDP	Tous	Communications via CAM sur le réseau
Gestionnaire de domaines	4104	Moteur de domaine distant	4104	UDP	Tous	Communications via CAM sur le réseau. Notifications, par exemple en cas d'évaluation de requête ad hoc
Explorateur	4104	N'importe quel moteur	4104	UDP	Tous	Communications via CAM sur le réseau
Serveur de modularité	4104	Moteur de domaine	4104	UDP	Tous	Communications via CAM sur le réseau

Ports utilisés par l'agent

Les tableaux suivants offrent un aperçu des ports utilisés pour les communications entre les agents.

Communications depuis l'agent

De	Port	A	Port	Protocole	Produit	Description
Agent	Non spécifiée	Agent	4105	TCP	Tous	Communications locales via CAM
Agent	4104	Serveur de modularité	4104	UDP	Tous	Communications via CAM sur le réseau
Agent	Non spécifiée	Serveur de modularité	4728	TCP	Tous	Transfert de fichiers non-NOS Transfert de données de sauvegarde
Agent	4104	Gestionnaire de domaines	4104	UDP	Remote Control Software Delivery	Communications via CAM sur le réseau Catalogue SD, Auth. Hôte RC, Visionneuse RC GAB
Agent	Ports de partage de fichiers	Serveur de modularité	Ports de partage de fichiers	TCP	Software Delivery	Transfert de fichiers de serveur NOS (Network Object Server)
Agent	554	Serveur de modularité	554	TCP	Software Delivery	RTSP (non sécurisé) pour des communications de diffusion en continu de Microsoft App-V
Agent	322	Serveur de modularité	322	TCP	Software Delivery	RTSPS (sécurisé) pour des communications de diffusion en continu de Microsoft App-V

Communications vers l'agent

De	Port	A	Port	Protocole	Produit	Description
Explorateur	4104	Agent	4104	UDP	Tous	Diagnostics instantanés (informations sur les composants DSM) Vérification des jobs déclencheur SD Vérification des jobs déclencheur AM
Serveur de modularité	4104	Agent	4104	UDP	Tous	Communications via CAM sur le réseau Configuration Vérification des jobs déclencheur SD Vérification des jobs déclencheur AM
Serveur de modularité	Non spécifiée	Agent	4728	TCP	Software Delivery	Transfert de fichiers DTS : transfert de package
Outil de packaging	Non spécifiée	Agent	3001, 3002	UDP	Tous	Localisateur du service DSM
Explorateur	Non spécifiée	Agent	4728 *)	TCP	Remote Control	Visionneuse RC vers hôte RC
Serveur de modularité	554	Agent	554	TCP	Software Delivery	RTSP (non sécurisé) pour des communications de diffusion en continu de Microsoft App-V
Serveur de modularité	322	Agent	322	TCP	Software Delivery	RTSPS (sécurisé) pour des communications de diffusion en continu de Microsoft App-V

Remarques :

- *) dans le tableau indique que l'hôte Remote Control écoutera également sur le port TCP 798 si le média de la visionneuse Remote Control héritée est activé.
- Un serveur de modularité peut être exécuté sur le même ordinateur qu'un gestionnaire de domaine.

Ports utilisés par la gestion de logiciels

Les tableaux suivants offrent un aperçu des ports utilisés pour les communications provenant de l'outil de packaging de logiciels.

Communications via l'outil de packaging :

De	Port	A	Port	Protocole	Produit	Description
Outil de packaging	4104	Gestionnaire d'entreprise	4104	UDP	Software Delivery	Données de contrôle d'enregistrement de package
Outil de packaging	Non spécifiée	Gestionnaire d'entreprise	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : Enregistrement du package
Outil de packaging	4104	Gestionnaire de domaines	4104	UDP	Software Delivery	Données de contrôle d'enregistrement de package
Outil de packaging	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : Enregistrement du package
Outil de packaging	Non spécifiée	Agent	3001, 3002	UDP	Tous	Localisation du service Client Automation

Ports utilisés par l'explorateur et le générateur de rapports DSM

Les tableaux suivants offrent un aperçu des ports utilisés pour les communications provenant de l'explorateur DSM et le générateur de rapports DSM vers l'explorateur DSM.

Communications depuis l'explorateur et le générateur de rapports

De	Port	A	Port	Protocole	Produit	Description
Explorateur	Non spécifiée	Explorateur	4105	TCP	Tous	Communications locales via CAM, Messages de notification

De	Port	A	Port	Protocole	Produit	Description
Explorateur	4104	Gestionnaire d'entreprise	4104	UDP	Tous	Communications via CAM sur le réseau
Explorateur	4104	Gestionnaire de domaines	4104	UDP	Tous	Communications via CAM sur le réseau
Explorateur	4104	Agent	4104	UDP	Tous	Diagnostics instantanés (informations sur les composants DSM) Vérification des jobs déclencheur SD Vérification des jobs déclencheur AM
Explorateur	4104	N'importe quel moteur	4104	UDP	Tous	Communications via CAM sur le réseau
Explorateur	Non spécifiée	Agent	4728	TCP	Remote Control	Visionneuse RC vers hôte RC
Explorateur	Ports de partage de fichiers	Gestionnaire d'entreprise	Ports de partage de fichiers	UDP	Software Delivery	Transfert de fichiers basé sur serveur NOS : enregistrement du package
Explorateur	Non spécifiée	Gestionnaire d'entreprise	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : enregistrement du package
Explorateur	Ports de partage de fichiers	Gestionnaire de domaines	Ports de partage de fichiers	TCP UDP	Software Delivery	Transfert de fichiers basé sur serveur NOS : enregistrement du package
Explorateur	Non spécifiée	Gestionnaire de domaines	4728	TCP	Software Delivery	Transfert de fichiers non-NOS : enregistrement du package

Communications vers l'explorateur

De	Port	A	Port	Protocole	Produit	Description
Gestionnaire de domaines	4104	Explorateur	4104	UDP	Tous	Communications via CAM sur le réseau
Gestionnaire d'entreprise	4104	Explorateur	4104	UDP	Tous	Communications via CAM sur le réseau

Ports utilisés par la passerelle ENC

Le tableau suivant offre un aperçu des ports utilisés pour les communications de la fonctionnalité Passerelle ENC.

De	Port	A	Port	Protocole	Produit	Description
Client ENC	Non spécifiée	Serveur de passerelle ENC	443	TCP	Tous	Enregistrement du client ENC, requêtes de connexion, requêtes d'écoute.
Client ENC	Non spécifiée	Serveur de passerelle ENC	80	TCP	Tous	Communications via CAM sur le réseau
Serveur de passerelle ENC	Non spécifiée	Serveur de passerelle ENC	443	TCP	Tous	Enregistrement du serveur de passerelle ENC, relais des requêtes clients au gestionnaire de passerelle ENC, relais des données entre les clients ENC connectés
Client ENC	Non spécifiée	Proxy Internet	1080	TCP	Tous	Communications via proxy
Client ENC	Non spécifiée	Proxy Internet	80	TCP	Tous	Communications via proxy

Ports utilisés par la quarantaine des actifs AMT

CA Client Automation (Client Automation) prend en charge la technologie AMT (Intel Advanced Management Technology). Dans ce contexte, une stratégie de quarantaine AMT est introduite, ce qui correspond à un disjoncteur ajoutant un filtre pour le trafic réseau entrant et sortant sur des dispositifs AMT.

La stratégie de quarantaine fournit un nouvel état de gestion pour les actifs AMT. Nous pouvons temporairement verrouiller ces actifs tout en réalisant une gestion avancée sur Client Automation. La stratégie de quarantaine ferme tout le trafic entrant et sortant normal, à l'exception des ports utilisés par les dispositifs AMT et Client Automation pour la communication, c'est-à-dire que les actifs Intel AMT en quarantaine peuvent être totalement gérées par Client Automation.

La stratégie de quarantaine affecte les ports comme suit :

- Trafic ARP Envoyer/Recevoir AMT depuis l'ordinateur AMT (port 67)
- Trafic de données Envoyer/Recevoir AMT sur les ports AMT (ports 16992 - 16995)
- Client Automation Envoyer/Recevoir sur port 4104

  Client Automation Envoyer/Recevoir sur port 4105

  Client Automation Envoyer/Recevoir sur port 4728
- Port de prise en charge pour le service DHCP où le port 53 est ouvert pour Recevoir.
- Port de prise en charge pour le service DNS où le port 63 est ouvert pour Envoyer/Recevoir.

Utilisation de port MDB

Les ports par défaut utilisés pour les communications MDB sont les suivants :

- Oracle : 1521
- Microsoft SQL Server : 1433

Une administrateur de base de données peut modifier les attributions de ports sur le site de la base de données.

Annexe C: Procédures Software Delivery pour l'installation

Le programme d'installation de CA Client Automation fournit un ensemble de procédures Software Delivery (SD) prédéfinies pour les packages d'installation.

Ce chapitre traite des sujets suivants :

Remarques importantes sur la procédure de désinstallation

Avant d'utiliser la procédure de désinstallation de l'agent Software Delivery (SD), remarquez ceci :

- La procédure de désinstallation du module d'extension de l'agent SD doit être exécutée en dernier dans le conteneur de jobs, car le module d'extension de l'agent SD effectue les jobs de désinstallation du package.
- Le module d'extension de l'agent de service de transport de données (DTS) étant un package différent sous Windows, la désinstallation de l'agent SD ne va pas de pair avec celle de l'agent DTS. L'agent DTS doit être désinstallé par un job distinct pouvant être incorporé au même conteneur de jobs.

Agent DSM CA + Module(s) d'extension AM, RC, SD Linux (Intel) ENU

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- programme d'installation
- Désinstallation complète de CA DSM

Agent CA DSM + module d'extension Asset Management Linux (Intel) ENU

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- programme d'installation
- Désinstallation complète de CA DSM
- Désinstaller uniquement le module d'extension Asset Management

Agent DSM CA + module d'extension d'inventaire de base Linux (Intel) ENU

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- programme d'installation
- Désinstallation complète de CA DSM

DMPrimer CA Linux (Intel) ENU

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- programme d'installation
- Désinstallation du logiciel d'injection de gestion d'ordinateurs de bureau autonomes

SMPackager (Linux)

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Installer le package
- Réinstaller le package
- Désinstaller le package

Supprimer l'agent hérité DSM CA Linux (Intel) ENU

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Suppression de tout
- Suppression de AM
- Suppression de SD

Agent DSM CA + Module d'extension Remote Control Linux (Intel) ENU

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Hôte géré de manière centralisée uniquement
- Agent autonome
- Désinstallation complète de CA DSM
- Désinstaller uniquement le module d'extension Remote Control

Agent DSM CA + Module d'extension Software Delivery Linux (Intel) ENU

Ce package d'installation inclut le module d'extension Data Transport.

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- programme d'installation
- Analyser les installations du programme d'installation SM
- Analyse de SWD
- Analyse de SWD : Logiciel Linux
- Programme d'installation SM : Désactiver le suivi
- Programme d'installation SM : Activer le suivi
- Programme d'installation SM : Obtenir tous les suivis
- Programme d'installation SM : Obtenir le dernier suivi
- Désinstallation complète de CA DSM
- Désinstaller uniquement le module d'extension Software Delivery

Serveur de modularité DSM CA Linux (Intel) ENU

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Désactivation du partage du serveur de démarrage
- Désactivation du partage MSILIB
- Désactivation du partage NFS
- Désactiver le partage Samba
- Désactivation du partage SDLIB
- Activation du partage du serveur de démarrage
- Activation du partage MSILIB
- Activation du partage NFS
- Activer le partage Samba
- Activation du partage SDLIB
- programme d'installation
- Synchronisation du calendrier CCS
- Synchronisation des enregistrements de jobs logiciels
- Synchronisation de la bibliothèque de transfert de logiciels
- Désinstallation complète de CA DSM
- Désinstaller uniquement Serveur de modularité + Agents

Agent DSM CA + Module(s) d'extension AM, RC, SD Win32

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Installer
- Désinstallation

Agent DSM CA + module d'extension Asset Management

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Détection
- Installer
- Réparation locale
- Désinstallation
- Vérification

Agent DSM CA + Module d'extension d'inventaire de base

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Détection
- Installer
- Réparation locale
- Désinstallation
- Vérification

Agent DSM CA + module d'extension Data Transport

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Détection
- Installer
- Réparation locale
- Désinstallation
- Vérification

Agent DSM CA + Module d'extension Remote Control

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Agent complet géré de manière centralisée
- Hôte géré de manière centralisée uniquement
- Détection
- Réparation locale
- Agent autonome
- Désinstallation
- Vérification

Agent DSM CA + Module d'extension Software Delivery

Ce package d'installation n'inclut pas le module d'extension Data Transport.

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Catalogue : Ajouter
- Catalogue : Supprimer
- Détection
- Diagnostics : Obtenir les informations de configuration et de version (informations dsmdiag)
- Installer
- Réparation locale
- Analyse de MSI (permet d'analyser la base de données MSI locale à la recherche de packages installés)
- Analyse des installations du programme d'installation SM (permet d'analyser les packages SXP installés sur l'agent)
- Analyse de SWD (analyse la base de données de l'agent propriétaire SD à la recherche de packages installés)
- Programme d'installation SM : Désactiver le suivi
- Programme d'installation SM : Activer le suivi
- Programme d'installation SM : Obtenir tous les suivis
- Programme d'installation SM : Obtenir l'historique
- Programme d'installation SM : Obtenir le dernier suivi
- Programme d'installation SM : Obtenir l'historique de l'utilisateur
- Programme d'installation SM : Obtenir le suivi de l'utilisateur
- Désinstallation
- Vérification

Constant Access DSM CA (Intel AMT)

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Installer
- Désinstallation

Explorateur DSM CA

Ce package d'installation contient les procédures liées à Software Delivery (SD) prédéfinies suivantes :

- Détection
- Installer
- Installation (sans Reporter)
- Installation d'AM
- Installation AM (sans Reporter)
- Installer AM + RC
- Installation AM + RC (sans Reporter)
- Installer AM + SD
- Installation AM + SD (sans Reporter)
- Installation d'RC
- Installation RC (sans Reporter)
- Installation d'SD
- Installation SD (sans Reporter)
- Installer SD + RC
- Installation SD + RC (sans Reporter)
- Réparation locale
- Désinstallation
- Vérification

Gestionnaire DSM CA

Ce package d'installation contient la procédure Software Delivery prédéfinie suivante :

- Détection

Serveur de modularité CA DSM

Le package d'installation du serveur de modularité dépend du package "Agent DSM CA + module d'extension Data Transport".

Le package Serveur de modularité contient les procédures Software Delivery prédéfinies suivantes :

- Détection
- Désactivation du partage du serveur de démarrage
- Désactivation du partage MSILIB
- Désactivation du partage SDLIB
- Activation du partage du serveur de démarrage
- Activation du partage MSILIB
- Activation du partage SDLIB
- programme d'installation
- Réparation locale
- Synchronisation du calendrier CCS
- Synchronisation des enregistrements de jobs logiciels
- Synchronisation de la bibliothèque de transfert de logiciels
- Désinstallation
- Vérification
- Désinstallation du serveur de modularité et des agents Software Delivery, Remote Control, Asset Management et des services de transport de données

Adaptateur de socket sécurisé DSM CA

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Installer
- Désinstallation

Suppression CA DSM de l'agent hérité Win32

Ce package d'installation contient les procédures Software Delivery prédéfinies suivantes :

- Suppression de AM
- Suppression de RC
- Suppression de SD
- Suppression de tout

Annexe D: Certificats actuels fournis par CA Client Automation

CA Client Automation fournit les certificats communs et propres aux applications répertoriés ci-dessous. Pour plus d'informations sur l'utilisation et la personnalisation des certificats, reportez-vous à "Comment introduire vos propres certificats X.509 dans l'image d'installation" (page 235) et à "Installation de certificats spécifiques à l'application" (page 417).

Ce chapitre traite des sujets suivants :

Certificats communs

Les certificats DSM communs sont les suivants :

Certificat racine DSM par défaut

DN:

CN=Racine DSM,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Racine DSM,O=Computer Associates,C=US

Certificat d'identité d'hôte standard par défaut

DN:

CN=Identité d'hôte générique,O=Computer Associates,C=US

URI :

x509cert://DSM r11/CN=Identité d'hôte générique,O=Computer Associates,C=US

Etiquette :

dsmcommon

Syntaxe :

Provision de certificat d'identité d'hôte standard.

Où :

Tous les noeuds dans l'entreprise.

Certificats propres aux applications

Les certificats propres aux applications sont utilisés pour affecter des autorisations de sécurité de niveau objet dans la base de données de gestion (MDB). Si vous créez de nouveaux certificats qui n'utilisent pas les noms par défaut, vous devez vous assurer que vous mettez le fichier cfcert.ini à jour avec les nouveaux URI avant l'installation du gestionnaire ou vous devez créer de nouveaux profils de sécurité possédant les droits et privilèges accordés aux profils de sécurité par défaut.

Veuillez vous reporter à la description présentée dans la section [Tags] du fichier cfcert.ini (page 237).

Certificat de synchronisation de répertoires

DN:

CN=Synchronisation des répertoires DSM,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Synchronisation des répertoires DSM,O=Computer Associates,C=US

Etiquette :

dsm_cmdir_eng

Syntaxe :

Pour permettre au job de moteur de synchronisation de répertoire de s'authentifier auprès d'un gestionnaire

Certificat d'enregistrement de serveur commun

DN:

CN=Enregistrement de serveur commun DSM,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Enregistrement de serveur commun DSM,O=Computer Associates,C=US

Etiquette :

dsm_csvr_reg

Syntaxe :

Enregistrement du gestionnaire et du serveur de modularité pour authentification auprès d'un gestionnaire.

Certificat de gestion de configuration et d'état

DN:

CN=Gestion d'état et de configuration,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Gestion d'état et de configuration,O=Computer Associates,C=US

Etiquette :

csm

Syntaxe :

Authentification du contrôleur d'agent CSM.

Certificat de déplacement d'agent Software Delivery

DN:

CN=Déplacement d'agent r11 DSM,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Déplacement d'agent r11 DSM,O=Computer Associates,C=US

Etiquette :

dsmagtmv

Syntaxe :

Déplacement d'agent Unicenter Software Delivery.

Où :

Noeuds de gestionnaire.

Certificat de catalogue Software Delivery

Nom unique :

CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

Balise :

dsmsdcat

Syntaxe :

Catalogue Software Delivery

Où :

Noeuds de gestionnaire, noeuds d'agent (Windows uniquement)

Remarques :

- Le certificat de catalogue Software Delivery dispose de droits en écriture (W) sur les ordinateurs et les profils d'utilisateur. Le certificat est présent sur tous les gestionnaires de domaines et les moteurs distants.
- Ne modifiez pas les autorisations de classe de profil d'utilisateur et d'ordinateur d'un certificat pour le gestionnaire de domaines ou l'un des moteurs distants.
- Ne supprimez pas le certificat par défaut, ni le certificat de catalogue Software Delivery spécifié par un utilisateur avec la même balise dsmsdcat.

Certificat d'accès à l'entreprise

DN:

CN=Accès à l'entreprise,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Accès à l'entreprise,O=Computer Associates,C=US

Etiquette :

ent_access

Syntaxe :

Accès par mot de passe à l'entreprise.

Certificat d'accès au domaine

DN:

CN=Accès à Domain,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Accès au domaine,O=Computer Associates,C=US

Etiquette :

dom_access

Syntaxe :

Accès par mot de passe au domaine.

Certificat d'accès au générateur de rapports

DN:

CN=Accès au générateur de rapports,O=Computer Associates,C=US

URI :

x509cert://dsm r11/CN=Accès au générateur de rapports,O=Computer Associates,C=US

Etiquette :

rep_access

Syntaxe :

Accès par mot de passe au générateur de rapports.

Annexe E: Cas d'utilisation de la prise en charge des zones de sécurité

Cette section traite des cas d'utilisation les plus importants dans le cadre de la prise en charge des zones du point de vue de l'utilisateur, puis décrit le fonctionnement de la prise en charge des zones.

Pour obtenir des informations de base sur la prise en charge des zones de sécurité et les autorisations de zone, reportez-vous aux sections Prise en charge des zones de sécurité (page 445) et Autorisations pour une zone (page 430).

Les descriptions des cas d'utilisation suivant la même structure, comme suit :

Scénario :

Fournit une brève explication du scénario utilisateur. Décrit ce qu'un utilisateur souhaite réaliser.

Pré-condition(s) :

Indique les objets qui sont définis avant que l'utilisateur n'effectue l'action décrite dans la section Action(s).

Action(s) :

Décrit ce qu'effectue un utilisateur.

Post-Condition(s) :

Définit les propriétés des objets impliqués dans le scénario, lorsque l'utilisateur a effectué l'action précédente.

Ce chapitre traite des sujets suivants :

Prise en charge de zones de sécurité pour les profils de sécurité

Les règles suivantes s'appliquent à la prise en charge de zones de sécurité pour les profils de sécurité :

- L'activation ou la désactivation de la prise en charge de zone de sécurité n'est pas permise pour le profil Tout le monde. L'accès à toutes les zones est refusé.
- Pour le profil Distributeur, vous devez disposer de l'accès complet à la classe de sécurité de prise en charge de zone de sécurité pour activer ou désactiver cette prise en charge.

Cas d'utilisation : Installation de Client Automation

Scénario :

Un utilisateur veut installer Client Automation.

Condition préalable :

Aucune version précédente de Client Automation n'a été installée sur l'ordinateur.

Action :

L'utilisateur installe Client Automation.

Conditions postérieures :

- Des profils intégrés par défaut sont installés.
- La prise en charge de zone est désactivée (paramètres globaux).
- Les autorisations de zone par défaut sont définies avec le paramètre Afficher toutes les zones.
- Le profil Tout le monde ne dispose d'aucun accès à quelque zone que ce soit.
- Le profil Administrateur dispose d'un accès complet à l'ensemble des zoneset ne peut être modifié.
- Aucune définition de zone prédéfinie n'a été installée.

Scénario d'utilisation : Mise à niveau d'une installation existante

Scénario :

Vous voulez mettre à niveau une installation existante.

Pré-condition :

Client Automation est installé.

Action :

Vous lancez l'installation de la MDB de DSM pour la mettre à niveau.

Post-conditions :

- Le schéma de MDB est modifié ou mis à niveau.
- La prise en charge de zone est désactivée après l'installation.
- Les paramètres area_aces sont créés pour tous les objets sécurisés existants pour lesquels la valeur est définie comme spécifiée dans les paramètres par défaut de l'indicatif régional.

Remarque : Après la mise à niveau, tous les objets sont affichés dans toutes les zones. Il s'agit de la configuration par défaut.

Cas d'utilisation : Profils de sécurité

Les importants scénarios d'utilisateur suivants concernant les profils de sécurité sont pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'un profil de sécurité (page 592)
- Modification de paramètres de zone pour un profil de sécurité (page 593)
- Suppression d'un profil de sécurité (page 593)

Cas d'utilisation : Création d'un profil de sécurité

Scénario :

Un administrateur veut créer un nouveau profil de sécurité.

Condition préalable :

Le profil de sécurité n'existe pas.

Action :

L'administrateur crée le nouveau profil de sécurité, où un ou plusieurs codes de zone sont affectés.

Conditions postérieures :

- Le profil de sécurité est créé.
- Toutes les autorisations au niveau de la classe de sécurité sont créées pour le nouveau profil de sécurité.
- L'autorisation au niveau de l'objet est calculée pour tous les objets sécurisés existants. Ces autorisations sont calculées pour les objets sécurisés existants (y compris les groupes). Les autorisations d'objet proviennent des autorisations au niveau de la classe.
- Des autorisations de zonesont crééeset dérivées d'autorisations de zone affectées au profil de sécurité.

Cas d'utilisation : Modification de paramètres de zone pour un profil de sécurité

Scénario :

Un administrateur souhaite modifier le code de zone attribué à un profil de sécurité.

Condition préalable :

Le profil de sécurité existe et une ou plusieurs zones sont affectées au profil.

Action :

L'administrateur modifie l'ancien code de zone d'un profil de sécurité par un nouveau.

Post-condition :

Les area_aces des objets sécurisésne sont pas modifiés.

Cas d'utilisation : Suppression d'un profil de sécurité

Scénario :

Un administrateur veut supprimer un profil de sécurité.

Condition préalable :

Le profil de sécurité existe et une ou plusieurs zones sont affectées au profil.

Action :

L'administrateur supprime le profil de sécurité.

Conditions postérieures :

- Le profil de sécurité est supprimé.
- Toutes les informations d'autorisation concernant les objets sécurisés et le profil de sécurité supprimé sont également supprimées.

Cas d'utilisation : Ordinateurs

Les importants scénarios d'utilisateur suivants concernant les ordinateurs sont pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création manuelle d'un ordinateur (page 594)
- Un nouvel agent DSM a été détecté (page 594)

Cas d'utilisation : Création manuelle d'un objet ordinateur

Scénario :

Un utilisateur veut créer un nouvel objet ordinateur.

Condition préalable :

Cet utilisateur est membre d'un ou de plusieurs profils de sécurité.

Action :

L'utilisateur crée le nouvel objet ordinateur à l'aide de l'explorateur DSM ou de l'utilitaire de ligne de commande DSM.

Conditions postérieures :

- Le nouvel objet ordinateur est créé.
- L'area_ace provient du profil de sécurité et est affecté à l'objet ordinateur. Si l'utilisateur est membre de plusieurs profils de sécurité, l'area_ace de tous les profils de sécurité est relié par l'opérateur OR et affecté à l'objet de sécurité.

Cas d'utilisation : Un nouvel agent DSM a été détecté

Scénario :

Un agent DSM a été déployé et s'exécute pour la toute première fois.

Condition préalable :

Il n'existe aucun objet dans la MDb pour la nouvelle ressource.

Action :

Aucune action de l'utilisateur. Le moteur DSM détecte le nouvel agent et crée l'objet de ressource (l'insère dans ca_discovered_hardware).

Conditions postérieures :

- Un objet sécurisé est créé.
- Les autorisations de zone sont affectées comme défini à un niveau global (paramètre de configuration global).

Cas d'utilisation : Groupes de ressources

Les importants scénarios d'utilisateur suivants concernant les groupes de ressources sont pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'un groupe de ressources (page 595)
- Ajout d'un ordinateur à un groupe de ressources (page 596)
- Suppression d'un ordinateur d'un groupe de ressources (page 597)
- Modification de l'autorisation de zone d'un groupe de ressources (page 598)
- Désactivation de l'héritage et du rétablissement (page 598)

Cas d'utilisation : Création d'un groupe de ressources

Scénario :

Un utilisateur souhaite créer un nouveau groupe de ressources où cet utilisateur est membre d'un seul profil de sécurité.

Condition préalable :

Il n'existe aucun groupe portant le même nom.

Action :

L'utilisateur crée le nouveau groupe de ressources.

Conditions postérieures :

- Le nouveau groupe est créé.
- Un group_ace est créé en fonction des autorisations de niveau de classe pour les groupes.
- Un object_ace est créé en fonction des autorisations de niveau de classe pour les groupes.
- L'area_ace est prélevé dans le profil de sécurité auquel appartient l'utilisateur de création. Si l'utilisateur de création est inconnu, l'area_ace par défaut est affecté.

Remarque : Cette même opération est valide pour les groupes de serveurs de modularité et les groupes de domaines.

Cas d'utilisation : Ajout d'un ordinateur à un groupe de ressources

Scénario :

Un utilisateur souhaite ajouter un ordinateur au groupe dont cet utilisateur est membre d'un seul profil de sécurité.

Pré-conditions :

- Le groupe de ressources existe.
- L'ordinateur existe.

Action :

L'utilisateur ajoute un ordinateur à un groupe ; l'héritage est activé pour le groupe.

Conditions postérieures :

- L'ordinateur est lié au groupe.
- S'il ne s'agit pas d'un groupe d'héritage, alors rien n'est effectué. S'il s'agit d'un groupe d'héritage, alors l'object_ace est calculé en fonction de l'object_ace sur le groupe parent.
- Le code de zone est défini comme suit :
  - Si l'ordinateur est uniquement membre d'un groupe de ressources, l'area_ace est identique à l'area_ace du groupe de ressources.
  - Si l'ordinateur est membre de plusieurs groupes de ressources, les area_aces des groupes parents sont liés par l'opérateur OR et affectés à l'objet sécurisé.

Variantes :

Si l'autorisation de zone de l'ordinateur est définie par le niveau creation_user ou le niveau par défaut global avant l'ajout au groupe, alors l'autorisation de zone est définie en fonction des autorisations de zone du groupe.

Si l'autorisation de zone de l'ordinateur est définie par le niveau object_level avant l'ajout au groupe, alors les autorisations de zone ne sont pas définies en fonction du niveau de groupe. L'utilisateur doit recourir à la fonction RETABLIR afin de recalculer les autorisations de zone en vue de la conformité avec le groupe.

Les autorisations de zone ne doivent pas changer si l'héritage d'une autorisation est désactivé.

Remarque : Cette même condition est valide dans le cas d'un groupe dynamique et du moteur effectuant l'évaluation du groupe. Dans ce cas, le moteur relie le membre au groupe.

Cas d'utilisation : Suppression d'un ordinateur d'un groupe de ressources

Scénario :

Un utilisateur souhaite supprimer un ordinateur d'un groupe de ressources où cet utilisateur est membre d'un ou de plusieurs profils de sécurité.

Pré-conditions :

- Le groupe de ressources existe.
- L'ordinateur existe.
- L'ordinateur est membre d'un seul groupe de ressources.

Action :

L'utilisateur supprime le lien entre l'ordinateur et le groupede ressources ; l'héritage est activé pour le groupe.

Conditions postérieures :

- Le lien reliant l'ordinateur au groupe est supprimé.
- Les autorisations de zone ne sont pas mises à jour.
- Le niveau de sécurité est défini selon le niveau d'objet.

Variantes :

Si l'ordinateurest membre de plus d'un groupe de ressources et que le niveau de sécurité est défini selon le niveau de groupe, alors les autorisations de zone sont recalculées (en fonction de l'affectation de groupe restante)et mises à jour.

Si l'autorisation de zone est définie sur le niveau d'objet, l'autorisation de zone n'est pas mise à jour.

Remarque : Après la suppression de l'ordinateur du groupe de ressources, l'utilisateur peut recourir à la fonction RETABLIR afin que les autorisations de zone de l'ordinateur soient au niveau de l'utilisateur de création.

Scénario d'utilisation : Modification des droits d'accès à une zone d'un groupe d'actifs

Scénario :

Vous voulez modifier les droits d'accès à une zone d'un groupe d'actifs existant.

Pré-conditions :

- Vous êtes associé à un ou plusieurs profils de sécurité.
- Le groupe d'actifs existe lorsque l'héritage d'autorisation est activé.

Action :

Vous utilisez la boîte de dialogue Modifier les autorisations pour associer ou annuler l'association d'une ou de plusieurs zones au groupe existant.

Post-conditions :

- Le paramètre area_ace du groupe existant est modifié.
- S'il s'agit d'un groupe hérité, le paramètre area_ace des membres est mis à jour.

Remarque : L'activation ou la désactivation de l'héritage des droits ne modifie pas les droits d'accès à la zone.

Cas d'utilisation : Désactivation de l'héritage et du rétablissement

Scénario :

Un utilisateur souhaite désactiver l'héritage d'un groupe de ressources et effectuer un rétablissement au niveau de laressource.

Pré-conditions :

- Un groupe de ressources existe là où l'héritage d'autorisation est activé.
- Unordinateur est lié au groupe de ressources, où des autorisations de zone sont définies au niveau de l'objet lors de la liaison.

Action :

L'utilisateur définit un héritage d'autorisation du groupe de ressources par désactivé, puis effectue un rétablissementpour l'objet ordinateur.

Post-condition :

Les autorisations d'objet de l'ordinateur sont rétablies en fonction de l'utilisateur de création.

Remarque : L'activation et la désactivation de l'héritage d'autorisation ne modifient pas les autorisations de zone.

Cas d'utilisation : Requêtes

Les importants scénarios d'utilisateur suivants concernant les requêtes sont pris en compte dans le cadre d'une prise en charge des zones de sécurité :

- Création d'une requête (page 599)
- Exécution d'une requête (page 600)
- Exécution d'une requêtes dans le contexte de Software Delivery (page 600)

Cas d'utilisation : Création d'une requête

Scénario :

Un utilisateur veut créer une nouvelle requête.

Condition préalable :

L'utilisateur est membre d'un seul profil de sécurité.

Action :

L'utilisateur crée la nouvelle requête.

Conditions postérieures :

- La nouvelle requête est créée.
- L'area_ace de la requête provient du profil de l'utilisateur de création de la requête.
- La nouvelle requête contient une condition where supplémentaire, afin de s'assurer que la requête renvoie uniquement des objets pour lesquels l'utilisateur de création dispose d'un accès (le même area_ace tel qu'affecté à la requête même).
- L'object_ace est créé en fonction de l'ace de niveau de classe de la classe de sécurité pour les requêtes.

Cas d'utilisation : Exécution d'une requête

Scénario :

Un utilisateur veut créer un groupe d'ordinateurs dynamique ; ce groupe doit être évalué par le moteur.

Condition préalable :

Aucune

Action :

Un utilisateur crée un groupe dynamique ; le groupe parent est Tous les ordinateurs.

L'utilisateurqui a créé la requête est différent de l'utilisateur qui a créé le groupe.

Conditions postérieures :

L'évaluation du groupe est effectuée par le moteur selon les règles suivantes :

- La requête est exécutée.
- Ajoutez uniquement ces ordinateurs en tant que membres du groupe correspondant à la même zone que celle de l'utilisateur qui a créé le groupe.

Cela signifie que les autorisations de zone de groupe disposent d'une priorité plus élevée que celle des autorisations de zone du groupe.

Cas d'utilisation : Exécution d'une requête dans le cadre de Software Delivery

Scénario :

Une requête est évaluée comme faisant partie d'une condition préalable de procédure Software Delivery. L'évaluation est effectuée par le gestionnaire de tâches Software Delivery.

Pré-condition :

Une procédure avec une condition préalable est utilisée pour l'installation sur un ordinateur cible et le paramètre de zone global est activé.

Action :

Le gestionnaire de tâches appelle l'API d'évaluation de requête, en transmettant l'utilisateur à partir de l'objet d'activité Software Delivery.

Post-condition :

La requête est évaluée dans le même contexte que ce lui de l'utilisateur qui a créé ce job dans l'interface utilisateur graphique (GUI). Cela signifie que la requête renvoie uniquement des objets dans la même zone que celle de l'utilisateur qui a créé le job. Si ce job a été créé par un processus en arrière-plan, où aucun contexte d'utilisateur n'était disponible, alors l'évaluation de requête renvoie tous les objets comme si la prise en charge de zone n'était pas activée.

Cas d'utilisation : Packages logiciels

L'important scénario d'utilisateur suivant concernant les packages logiciels est pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'un package logiciel (page 601)

Cas d'utilisation : Création d'un package logiciel

Scénario :

Un utilisateur veut créer un nouveau package logiciel.

Condition préalable :

Ce package logiciel n'existait pas.

Action :

L'utilisateur crée le package logiciel à l'aide du GUI Client Automation.

Conditions postérieures :

- Le package logiciel est créé.
- Des autorisations de zone sontcréées et le package logiciel est lié aux mêmes zones que celles de l'utilisateur qui a créé l'objet.

Cas d'utilisation : Procédures logicielles

L'important scénario d'utilisateur suivant concernant les procédures logicielles est pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'une procédure logicielle (page 601)

Cas d'utilisation : Création d'une procédure logicielle

Scénario :

Un utilisateur veut créer une nouvelle procédure logicielle.

Condition préalable :

Cette procédure logicielle n'existait pas.

Action :

L'utilisateur crée la procédure logicielle à l'aide du GUI Client Automation.

Post-condition :

Cette procédure hérite des mêmes autorisations de zone que celles du package logiciel dans lequel elle est incluse.

Cas d'utilisation : Groupes de logiciels

L'important scénario d'utilisateur suivant concernant les groupes de logiciels est pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'un groupe de logiciels (page 602)

Cas d'utilisation : Création d'un groupe de logiciels

Scénario :

Un utilisateur veut créer un nouveau groupe de logiciels.

Condition préalable :

Cet utilisateur est membre d'un ou de plusieurs profils de sécurité.

Action :

L'utilisateur crée le nouveau groupe de logiciels à l'aide de l'explorateur DSM (un nouveau noeud sous la bibliothèque de packages logiciels).

Conditions postérieures :

- Le nouveau groupe de logiciels est créé.
- L'area_ace du groupe de logiciels provient du profil de l'utilisateur de création de la requête.
- L'objects_ace est créé en fonction de l'ace de niveau de classe de la classe de sécurité pour les jobs de ressource.
- Un group_ace est également créé en fonction de l'ace de niveau de classe du profil de sécurité.

Cas d'utilisation : Stratégies logicielles

L'important scénario d'utilisateur suivant concernant les stratégies logicielles est pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'une stratégie logicielle (page 603)

Cas d'utilisation : Création d'une stratégie logicielle

Scénario :

Un utilisateur veut créer une nouvelle stratégie logicielle.

Pré-condition :

Cet utilisateur est membre d'un ou de plusieurs profils de sécurité.

Action :

L'utilisateur crée la nouvelle stratégie logicielle à l'aide de l'explorateur DSM ou de la ligne de commande Client Automation.

Post-conditions :

- La nouvelle stratégie logicielle est créée.
- La stratégie logicielle est affectée au groupe d'actifs.
- L'object_ace est dérivé de l'ace de sélection de classe.
- Les autorisations de zone de la stratégie logicielle proviennent du profil de l'utilisateur ayant créé la stratégie.

Cas d'utilisation : Jobs logiciels

L'important scénario d'utilisateur suivant concernant les jobs logiciels est pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'un job logiciel (page 603)

Cas d'utilisation : Création d'un job logiciel

Scénario :

Un utilisateur veut créer un nouveau job logiciel.

Pré-condition :

Cet utilisateur est membre d'un ou de plusieurs profils de sécurité.

Action :

L'utilisateur crée la nouvelle stratégie logicielle à l'aide de l'explorateur DSM ou de la ligne de commande DSM.

Post-conditions :

- Le nouveau job logiciel est créé.
- Les autorisations d'objet proviennent de l'ace de sélection de classe.
- Les autorisations de zone du job logiciel proviennent du profil de l'utilisateur ayant créé le job.

Cas d'utilisation : Jobs de ressources

L'important scénario d'utilisateur suivant concernant les jobs de ressource est pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Création d'un job de ressource (page 604)

Cas d'utilisation : Création d'un job de ressource

Scénario :

Un utilisateur veut créer un nouveau job de ressource.

Condition préalable :

L'utilisateur est membre d'un seul profil de sécurité.

Action :

L'utilisateur crée le nouveau job de ressource. Le type du job de ressource peut être de n'importe quel type, tel que messages, commande, etc.

Conditions postérieures :

- Le nouveau job de ressource est créé.
- L'area_ace du job de ressource provient du profil de l'utilisateur de création de la requête.
- L'objects_ace est créé en fonction de l'ace de niveau de classe de la classe de sécurité pour les jobs de ressource.

Cas d'utilisation : tâches de moteur

Le scénario d'utilisateur suivant concernant les tâches de moteur est considéré dans le cadre d'une prise en charge de zone de sécurité :

- Création d'une tâche de moteur (page 605)

Cas d'utilisation : création d'une tâche de moteur

Scénario :

Un utilisateur veut créer une tâche de moteur.

Condition préalable :

L'utilisateur est membre d'un seul profil de sécurité.

Action :

L'utilisateur crée la tâche de moteur

Conditions postérieures :

- La nouvelle tâche de moteur est créée.
- L'autorisation de zone de la tâche de moteur provient du profil de l'utilisateur ayant créé la tâche de moteur.
- Les autorisations d'objet sont créées en fonction de l'autorisation de niveau de classe de la classe de sécurité pour les jobs de ressources.

Cas d'utilisation : Gestion de zones

Les importants scénarios d'utilisateur suivants concernant la gestion de zones sont pris en compte dans le cadre d'une prise en charge de zone de sécurité :

- Première activation de la prise en charge de code de zone (page 606)
- Désactivation de la prise en charge de code de zone (page 606)
- Réactivation de la prise en charge de code de zone (page 607)
- Modification des autorisations de zone par défaut (page 607)
- Ajout d'une nouvelle zone (page 608)
- Suppression d'une zone (page 608)

Cas d'utilisation : Première activation de la prise en charge de code de zone

Scénario :

Un administrateur veut activer le code de zone pour tous les profils de sécurité alors que celui-ci était désactivé auparavant.

Pré-conditions :

- La prise en charge du code de zone est désactivée et le produit Client Automation a déjà été utilisé.
- Des objets et des profils sécurisés ont été créés alors que la prise en charge de zone était désactivée.

Action :

L'administrateur active la prise en charge de code de zone.

Conditions postérieures :

- La prise en charge du code de zone est activée dans la MDB.
- Les codes de zone de tous les profils sont définis en fonction du code de zone par défaut, comme défini lors de la création du profil de sécurité.
- Les codes de zone de tous les objets sécurisés existants sont définis en fonction des codes de zone, comme défini pour le profil de sécurité.

Remarque : Cela signifie qu'un administrateur doit affecter explicitement un ou plusieurs codes de zone au profil de sécurité après la première activation de la prise en charge du code de zone.

Cas d'utilisation : Désactivation de la prise en charge de code de zone

Scénario :

Un administrateur souhaite désactiver les codes de zone de tous les profils de sécurité.

Condition préalable :

Les codes de zone sont correctement définis dans la MDB.

Action :

L'administrateur désactive la prise en charge de code de zone.

Conditions postérieures :

- L'indicateur dans la MDB est défini de manière à désactiver le code de zone.
- Le code de zone même n'est pas supprimé ni modifié.

Cas d'utilisation : Réactivation de la prise en charge de code de zone

Scénario :

Un administrateur souhaite activer à nouveau le code de zone de tous les profils de sécurité.

Condition préalable :

Les codes de zone sont correctement définis dans la MDB, mais la prise en charge de code de zone est définie par DESACTIVEE.

Action :

L'administrateur active la prise en charge de code de zone.

Conditions postérieures :

- L'indicateur dans la MDB est défini de manière à activer le code de zone.
- Le code de zone lui-même est identique à la période avant la désactivation de la prise en charge du code de zone.

Scénario d'utilisation : Modification des droits d'accès à une zone par défaut

Scénario :

Vous voulez modifier les droits d'accès à une zone par défaut.

Pré-condition :

Client Automation est installé.

Action :

Vous modifiez les autorisations par défaut.

Post-conditions :

- Les droits d'accès à la zone par défaut, tels qu'ils sont stockés dans la MDB, sont modifiés.
- Tous les droits d'accès à la zone où le niveau de sécurité est défini sur la valeur par défaut sont également modifiés.

Cas d'utilisation : Ajout d'une nouvelle zone

Scénario :

Un utilisateur veut créer une nouvelle définition de zone.

Condition préalable :

L'utilisateur est membre d'un profil de sécurité. La classe de sécurité pour contrôler la prise en charge de zone (SEC_CLSID_COM_CONTROL_AREA)permet au moins la création d'une nouvelle zone.

Action :

L'utilisateurcrée la nouvelle définition de zone.

Post-condition :

La nouvelle zoneest créée.

Cas d'utilisation : Suppression d'une zone

Scénario :

Un utilisateur veut supprimer une définition de zone.

Condition préalable :

L'utilisateur est membre d'un profil de sécurité. La classe de sécurité pour contrôler la prise en charge de zone (SEC_CLSID_COM_CONTROL_AREA)permet au moins la suppression d'une zone.

Action :

L'utilisateur supprime la définition de zone manuellement.

Conditions postérieures :

- La zoneest supprimée.
- Des autorisations de zone sont mises à jour pour indiquer que la zone n'existe plus.

Cas d'utilisation : S'approprier

L'appropriation ne modifie pas l'autorisation de zone de quelque objet que ce soit.

Annexe F: Jobs planifiés CAF

Les règles complètes de spécification des jobs planifiés qui sont exécutés dans le cadre d'applications communes (CAF) sont décrites ci-après. Ces jobs couvrent l'exécution des commandes caf à intervalles réguliers ou aléatoires. Par exemple, il existe un job standard qui exécute l'agent Asset Management une fois par jour.

Ce chapitre traite des sujets suivants :

Jobs et paramètres standard CAF

CAF est installé avec un ensemble de jobs standard (pour plus de détails, consultez le Groupe de stratégies CAF dans la section Stratégie de configuration dans *Aide de l'explorateur DSM*).

Un job est décrit par un ensemble de paramètres stockés dans le magasin de configuration (comstore) sous la clé :

`itrm/common/caf/scheduler/`*`nom_du_job`*

Le planificateur proprement dit peut être activé ou désactivé en définissant le paramètre enabled (activé) dans la clé ci-dessus.

Un job présente les paramètres suivants:

Description

Définit la description du job. Elle apparaît dans les journaux de suivi.

activé

Indique si un job est activé. Les valeurs valides sont les suivantes : 1=le job est activé, 0= le job n'est pas activé et ne sera pas exécuté.

type

Spécifie le type de job. Ce paramètre détermine l'intervalle de temps auquel le job se répète et peut présenter l'une des valeurs suivantes :

jour

Exécute le job tous les quelques jours à une heure donnée exacte (minutes incluses).

heure

Exécute le job toutes les quelques heures à une minute donnée de l'heure.

minute

Exécute le job toutes les quelques minutes.

Vous pouvez également spécifier les mots-clés supplémentaires suivants :

maintenant

Exécute le job immédiatement et aux intervalles planifiés par la suite. Dans ce contexte, le terme now signifie Au démarrage de caf.

Si le paramètre randomnowtime (délai immédiat aléatoire) est défini, le job est exécuté dans un délai aléatoire qui va de plusieurs secondes jusqu'à la valeur définie pour randomnowtime. Ceci permet de s'assurer que les ordinateurs qui démarrent ensemble ne lancent pas tous leurs job au même moment.

random

Exécute le job à un moment spécifié auquel est ajouté un nombre aléatoire de minutes qui va jusqu'à la valeur définie pour le paramètre randomminutes (minutes aléatoires). Ce paramètre est utilisé dans les jobs qui impliquent un contact avec les serveurs. Ceci aide à répartir la charge sur les serveurs en rendant partiellement aléatoire le moment auquel les agents prennent contact.

random_hour

Spécifie l'exécution du job à une heure aléatoire du jour. Utilisé avec les planifications quotidiennes.

random_minute

Spécifie l'exécution du job à une minute aléatoire dans l'heure définie (qui peut aussi être aléatoire). Utilisé avec les planifications quotidiennes et horaires.

excludeDays

Spécifie les noms des jours à exclure de la planification : lundi, mardi, etc. Séparez chaque jour par des espaces. Par exemple, le paramètre "lundi mercredi" empêche l'exécution du job le lundi et le mercredi.

excludeHours

Spécifie les nombres des heures à exclure de la planification, sur la base d'une horloge de 24 heures. Séparez chaque heure par des espaces. Par exemple, le paramètre "1 15" empêche l'exécution du job à 1 heure et 3 heures du matin.

heure

Spécifie l'heure à laquelle le job démarre au format horaire 24 heures. Ce paramètre s'utilise avec les planifications quotidiennes uniquement.

minute

Spécifie la minute à laquelle le job démarre dans l'heure. Ce paramètre s'utilise avec les planifications quotidiennes et horaires.

repeat

Répète chaque unité de temps définie par la propriété type. Par exemple, si type est défini sur hour (heure), alors repeat (répéter) spécifie le nombre d'heures entre les jobs.

randomnowtime

Indique un nombre de secondes. Au démarrage de CAF, un job identifié par now est exécuté à un moment aléatoire compris dans ce nombre de secondes.

randomminutes

Indique un nombre de minutes. Le job est exécuté à un moment spécifié auquel est ajouté un délai aléatoire qui va jusqu'à la valeur définie pour ce paramètre.

cmd

Spécifie la commande caf permettant l'exécution de ce job. cmd est identique à la ligne de commande, à ceci près que les options concernant l'hôte, l'utilisateur et le mot ne passe ne peuvent pas être utilisés.

Exemples de jobs planifiés CAF

Exemple : Exécuter le module d'extension amagent toutes les heures

```
type=”hour”, repeat=1, minute=0, cmd=”start amagent”
```

Exemple : Exécuter l'amagent chaque jour à 14h30

```
type=”day”, repeat=1, hour=14, minute=30, cmd=”start amagent”
```

Exemple : Exécute l'amagent lors du démarrage de CAF et ensuite chaque jour à une heure quelconque entre 1 heure et 2h30, sauf durant le week-end

```
type=”day now random”, hour=1, minute=0, randomminutes=90, excludedays=”saturday
sunday”, cmd=” start amagent”
```

Annexe G: Conformité à la norme FIPS 140-2

Cette annexe présente en détail l'utilisation de la cryptographie dans CA ITCM, notamment le niveau de conformité aux normes de publication FIPS 140-2.

Ce chapitre traite des sujets suivants :

Norme FIPS PUB 140-2

La norme FIPS 140-2 est une norme de sécurité qui spécifie les exigences de sécurité pour un module cryptographique utilisé au sein d'un système de sécurité. Il s'agit d'une norme fournie par le NIST (National Institute of Standards and Technology) pour évaluer et accréditer le fonctionnement de modules cryptographiques via le Programme de validation des modules cryptographiques (CMVP, Cryptographic Module Verification Program). Le CMVP est exécuté par des laboratoires de test certifiés par le NIST pour tester et valider des modules cryptographiques. Les modules sont testés par rapport aux exigences de test dérivées de la norme FIPS 140-2.

Pour chaque fonction de sécurité validée et approuvée pour l'utilisation en mode accrédité par la norme FIPS 140-2, un certificat correspondant au Programme de validation des algorithmes cryptographiques (Cryptographic Algorithm Validation Program, CAVP) est enregistré dans le certificat d'approbation de la norme FIPS 140-2 pour le module. Ce certificat répertorie toutes les fonctions de sécurité fournies par le module, qu'elles soient ou non approuvées, et détaille les fonctions pouvant être utilisées en mode de fonctionnement approuvé par la norme FIPS 140-2.

Chaque module approuvé publie un document de stratégie de sécurité associé, expliquant le fonctionnement du module pour être conforme à la norme FIPS 140-2.

Remarque : Seuls les modules cryptographiques peuvent être certifiés comme étant accrédités et approuvés par la norme FIPS 140-2. Ce n'est pas le cas des applications, bien qu'elles puissent utiliser des modules approuvés par la norme FIPS 140-2 et dont le mode de fonctionnement est également approuvé.

Références

Pour plus d'informations sur le programme CMVP, visitez le site Web du NIST :

http://csrc.nist.gov/groups/STM/cmvp/

Pour en savoir plus sur les modules validés et les liens vers leurs stratégies de sécurité correspondantes, visitez la page :

http://csrc.nist.gov/groups/STM/cmvp/validation.html

Vous trouverez des informations relatives aux numéros de certificat référencés dans cette annexe dans l'URL mentionnée ci-dessus.

Modes FIPS pris en charge

Client Automation peut fonctionner dans l'un des modes suivants :

Préférence FIPS

En mode Préférence FIPS, Client Automation préfère utiliser les fonctions de sécurité approuvées par la norme FIPS 140-2. Toutefois, lorsqu'il communique avec des composants Client Automation hérités, il utilise des fonctions de sécurité héritées. Les modules cryptographiques incorporés ne fonctionnent *pas* en modes accrédités par la norme FIPS 140-2, car ils requièrent l'utilisation de fonctions de sécurité non approuvées (par ex., MD5). Lorsqu'il fonctionne en mode Préférence FIPS, Client Automation peut communiquer et interagir avec les versions précédentes de Client Automation.

FIPS uniquement

En mode FIPS uniquement, Client Automation utilise *uniquement* des fonctions de sécurité approuvées par la norme FIPS 140-2. Les fonctions de sécurité non approuvées peuvent être utilisées de manière non cryptographique, tel qu'indiqué dans les sections ci-dessous, mais en mode de fonctionnement approuvé par la norme FIPS 140-2, elles ne sont fournies par aucun module cryptographique incorporé. Dans ce mode, Client Automation peut uniquement interagir avec les composants conformes à la norme FIPS, soit en mode Préférence FIPS, soit en mode FIPS uniquement.

Remarque : Cette annexe porte sur l'utilisation de la cryptographie lorsque Client Automation fonctionne en mode FIPS uniquement.

Module cryptographique RSA Crypto

Client Automation utilise directement et incorpore les modules cryptographiques suivants :

- RSA Crypto-C ME Version 2.1 ; Certificat CMVP #828

Voici un extrait de la stratégie de sécurité de ce module cryptographique :

"Ce module cryptographique est classé comme module autonome multipuce à des fins de conformité avec la norme FIPS 140-2. En tant que tel, le module doit être testé dans un système d'exploitation et une plate-forme informatique particuliers. Ainsi, la limite cryptographique inclut le module cryptographique exécuté sur des plates-formes sélectionnées exécutant des systèmes d'exploitation sélectionnés lors de la configuration en mode Utilisateur unique. Le module cryptographique a été validé, car il réunit toutes les conditions de sécurité de niveau 1 de la norme FIPS 140-2 1, y compris la gestion de clés de chiffrement et la configuration requise des systèmes d'exploitation. Le module cryptographique est mis en package comme module dynamiquement chargé ou comme fichier de bibliothèque partagé, contenant tous les codes exécutables du module. De plus, la boîte à outils RSA BSAFE Crypto-C ME utilise la sécurité physique fournie par le PC hôte sur lequel elle est exécutée."

Fonctions cryptographiques de sécurité

Le tableau suivant fournit les algorithmes cryptographiques du module Crypto-C RSA utilisés par Client Automation pour diverses fonctions de sécurité :

Fonction de sécurité	Algorithme cryptographique	Numéro de certificat de validation	Commentaires
Chiffrement et déchiffrement asymétriques	Chiffrer ou déchiffrer avec RSA	Non approuvé	Autorisé en mode FIPS 140-2 pour le transport de clés
Chiffrement et déchiffrement symétriques	AES CBC	490	FIPS PUB 197 - Advanced Encryption Standard
	Triple-DES	510	FIPS PUB 46-3 - Data Encryption Standards FIPS SP 800-67 - Recommandation pour le Triple Data Encryption Algorithm (TDEA) Block Cipher ANSI X9.52 - TDEA approved modes of operation
Fonctions de hachage	SHA-1	560	FIPS PUB 180-3 – Secure Hash Standard

Fonction de sécurité	**Algorithme cryptographique**	**Numéro de certificat de validation**	**Commentaires**
	SHA-256	560	FIPS PUB 180-3 – Secure Hash Standard
	SHA-512	560	FIPS PUB 180-3 – Secure Hash Standard
Génération aléatoire de numéros	PRNG	270	FIPS PUB 186-2 – Digital Signature Standard Pour plus d'informations, consultez l'annexe 3 : Génération aléatoire de numéros de DSA dans le document sur la Norme de signature numérique de FIPS PUB 186-2.
Etablissement de clé asymétrique	TLS 1.0	Non applicable	Autorisé par le document de manuel d'implémentation de la norme FIPS 140-2 contenant des suites de chiffrement approuvées par la norme FIPS
	SSH v2	Non applicable	Autorisé par le document de manuel d'implémentation de la norme FIPS 140-2 contenant des suites de chiffrement approuvées par la norme FIPS

Utilisation cryptographique propre aux composants

Cette section présente l'utilisation cryptographique propre aux composants lorsque Client Automation fonctionne en mode FIPS uniquement :

Communications entre les noeuds [Messagerie de session]

Le composant de messagerie de session utilise le protocole TLS v1.0 pour la communication entre les noeuds. La suite de chiffrement choisie sera sélectionnée suite à la négociation entre les noeuds communiquant.

Dans certaines instances, le composant de messagerie de session utilise la structure des informations sur le destinataire du transport de clés, telle que spécifiée dans la version de la syntaxe de message cryptographique 3 (CMS3), telle qu'indiquée en RFC3369.

Mise en réseau basée sur le flux

Le composant de mise en réseau basé sur le flux utilise le protocole TLS v1.0 pour des communications entre les noeuds. La suite de chiffrement choisie sera sélectionnée suite à la négociation entre les noeuds communiquant.

Remote Control - Carnet d'adresses local

Les entrées du carnet d'adresses local Remote Control sont protégées par l'algorithme 3TDES en mode CBC avec vecteur d'initialisation aléatoire.

Desktop Migration Manager [DMM]

DMM utilise le protocole de TLS v1.0 pour la communication et l'algorithme AES avec des clés de 192 bits en mode CBC avec vecteur d'initialisation aléatoire.

ENC

La fonctionnalité ENC fournie dans Client Automation étant actuellement disponible uniquement sous Windows, elle est étroitement intégrée au fournisseur Microsoft SCHANNEL (Magasin de certificats Microsoft) et par conséquent au fournisseur de services cryptographiques Microsoft sous-jacent (RSAENH). Pour plus d'informations sur le statut FIPS des fournisseurs de services cryptographiques Microsoft, consultez la section Environnements d'exploitation Windows certifiés FIPS (page 619).

OSIM et Software Delivery

OSIM et Software Delivery utilisent le chiffrement symétrique fourni par l'algorithme AES en mode de CBC avec vecteur d'initialisation aléatoire et structuré à l'aide de la version 3 de la syntaxe de message cryptographique (CMS3), tel qu'indiqué dans RFC3369.

Gestionnaire d'objets communs, Moteur commun, Outil d'extraction SMS

Les composants de gestionnaire d'objets communs, moteur commun et Outil d'extraction SMS utilisent l'algorithme 3TDES en mode CBC avec vecteur d'initialisation aléatoire.

Virtualisation de plates-formes - Module ESX

Le module ESX utilise le protocole de TLS v1.0 pour la communication avec des noeuds VMware ESX distants.

DTS

Les programmes DTS utilisent le chiffrement symétrique fourni par l'algorithme AES ou par 3TDES, avec des tailles de clés variables, mais tout en utilisant le mode CBC avec vecteurs d'initialisation aléatoires.

CCS

Client Automation peut utiliser CA Common Services (que vous pouvez installer). Pour obtenir une description détaillée du niveau de conformité de CA Common Services à la norme FIPS, consultez la section Chiffrement conforme à la FIPS 140-2 de l'annexe B du *Manuel d'administration CA NSM* disponible dans la bibliothèque CA.

Conformité FIPS des composants externes à Client Automation

Il existe de nombreuses autres utilisations de la cryptographie dans un ordinateur, externes aux applications Client Automation.

Environnements d'exploitation Windows

Le fournisseur de services cryptographiques avancés Microsoft [RSAENH CSP] est certifié FIPS-140 pour divers environnements d'exploitation Windows. Pour obtenir une liste de ces environnements d'exploitation certifiés FIPS, consultez le document http://technet.microsoft.com/en-us/library/cc750357.aspx. Ce lien contient également des détails sur l'activation de la stratégie de sécurité locale pour l'utilisation de la cryptographie conforme à la norme FIPS. Pour qu'ENC soit conforme à la norme FIPS, vous devez configurer la stratégie de sécurité locale (Cryptographie du système : utilisation d'algorithmes conformes à la norme FIPS pour le chiffrement, le hachage et la signature).

Remarque : Vous devez soigneusement prendre en compte l'impact du fonctionnement en mode FIPS uniquement et autoriser le chiffrement conforme à la FIPS uniquement. Pour plus d'informations, consultez la rubrique Prise en charge de la norme FIPS 140-2 (page 86).

SQL Server

La version 2005 SP1 de Microsoft SQL Server est conforme à la-FIPS. Pour plus d'informations sur la configuration du serveur SQL en mode conforme à la FIPS, consultez l'entrée 920955 de la base de connaissances Microsoft à l'adresse : http://support.microsoft.com/kb/.

Autres composants

Client Automation est une suite d'applications et de modules de composants qui fournit une solution professionnelle. En tant que package logiciel, Client Automation utilise également des composants et des services appartenant à d'autres groupes CA et à des fournisseurs tiers. Sauf indication contraire, aucun de ces composants et/ou services n'implémente ni n'expose des fonctionnalités cryptographiques directement à Client Automation et, par conséquent, leur conformité avec les modules cryptographiques certifiés FIPS 140-2 n'est pas documentée. Pour obtenir des informations concernant la FIPS 140-2, consultez la documentation auprès des fournisseurs des composants.

En outre, les opérations cryptographiques au sein de systèmes d'exploitation incombent aux fournisseurs de systèmes d'exploitation. Pour obtenir des informations sur la FIPS 140 et la prise en charge des critères communs, y compris le niveau de conformité et/ou toute exigence de configuration prise en charge, consultez la documentation relative à la FIPS 140-2 auprès des fournisseurs.

Remarque : Pour obtenir la dernière liste mise à jour des composants fournis avec Client Automation, consultez la matrice de compatibilité.

Utilisation non approuvée des fonctions de sécurité

Dans certains cas, Client Automation utilise des fonctions de sécurité non autorisées par la publication de la FIPS 140-2. Celles-ci n'ont aucune conséquence sur le fonctionnement de Client Automation en mode FIPS-uniquement.

Agent Asset Management - Analyseur de signatures logicielles

Lorsqu'une signature logicielle contient une valeur d'attribut de "md5" pour une balise <file>, l'analyseur de signatures utilise une implémentation privée du code MD5. L'analyseur vérifie si l'algorithme MD5 d'un fichier situé sur l'ordinateur agent correspond à l'attribut "md5" avant de renvoyer un résultat positif pour cette signature. L'analyseur de signatures logicielles n'utilisent pas le MD5 à des fins cryptographiques.

Installation

Pendant l'installation de Client Automation, vous pouvez utiliser les fichiers PKCS#12 pour l'installation du certificat et de la clé. Ces fichiers sont chiffrés à l'aide d'une clé résultant d'une fonction de dérivation de clé de mot de passe (PBKD), par exemple PBKDF2 à partir de la norme PKCS#5 v2.0. Pendant l'installation, ces fichiers sont extraits et protégés à l'aide de techniques non basées sur le mot de passe.

Remarque : La dérivation de clé de mot de passe (établissement de la clé basée sur le mot de passe) est explicitement rejetée aux fins de l'accord de clé asymétrique, tel qu'indiqué à la section 7.1 du document de Conseils d'implémentation de la FIPS 140-2.

Annexe H: Fonctionnalités d'accessibilité

CA Technologies s'engage à rendre possible l'utilisation, par tous ses clients et indépendamment de leurs aptitudes, des produits CA et de la documentation qui les accompagne dans le cadre de la réalisation des tâches cruciales liées à leurs activités. Cette section décrit les fonctionnalités d'accessibilité incluses dans Client Automation.

Ce chapitre traite des sujets suivants :

Annexe I: Améliorations du produit

Client Automation propose des améliorations d'accessibilité dans les domaines suivants :

- Affichage
- Son
- Clavier
- Souris

Remarque : Les informations suivantes s'appliquent aux applications Windows et Macintosh. Les applications Java s'exécutent sur différents systèmes d'exploitation hôtes, certains possédant déjà des technologies d'assistance. Pour que ces technologies d'assistance existantes permettent d'accéder aux programmes écrits en JPL, un pont doit les relier dans leurs environnements natifs et l'accessibilité Java disponible à partir de la machine virtuelle Java (VM) doit être prise en charge. Ce pont dispose d'une extrémité sur la machine virtuelle Java et d'une autre extrémité sur la plate-forme native, c'est pourquoi il varie légèrement selon la plate-forme à laquelle il est relié. Sun développe actuellement les côtés JPL et Win32 de ce pont.

Affichage

Pour augmenter la visibilité sur l'écran de votre ordinateur, vous pouvez ajuster les options suivantes.

- Style, couleur et taille de police d'éléments

  Permet de sélectionner la couleur et la taille des polices ainsi que d'autres combinaisons visuelles.

- Résolution d'écran

  Permet de changer le nombre de pixels pour agrandir des objets sur l'écran.

- Largeur de curseur et fréquence de clignotement

  Permet de rendre le curseur plus visible ou de réduire son clignotement.

- Taille des icônes

  Permet d'agrandir les icônes pour une meilleure visibilité ou de les réduire pour augmenter l'espace sur l'écran.

- Schémas de contraste élevé

  Permet de sélectionner des combinaisons rendant les couleurs plus faciles à voir.

Remarques :

- Si vous souhaitez activer l'interface utilisateur distincte pour des systèmes d'exploitation antérieurs à Windows Vista, plutôt que d'utiliser l'interface utilisateur graphique actuelle, appliquez la stratégie de configuration Software Delivery, Agent, Toujours afficher l'interface utilisateur graphique pour les utilisateurs connectés.
- Pour activer les technologies assistives afin de lire le texte dans la fenêtre de vérification des jobs SD sur des systèmes d'exploitation antérieurs à Windows Vista, appliquez à l'agent la stratégie de configuration Software Delivery, Agent, Toujours afficher l'interface utilisateur graphique pour les utilisateurs connectés.

Son

Permet de remplacer les méthodes visuelles par du son ou d'ajuster les options de son suivantes de l'ordinateur afin de les rendre plus audibles ou de mieux les distinguer.

- Volume

  Permet d'augmenter ou de baisser le son.

- Conversion de texte par synthèse vocale

  Permet d'entendre les options de commande et le texte lu à haute voix.

- Avertissements

  Permet d'afficher des avertissements visuels.

- Notifications

  Fournit des indications auditives ou visuelles lorsque les fonctionnalités d'accessibilité sont activées ou désactivées.

- Schémas

  Permet d'associer des sons de l'ordinateur avec des événements système spécifiques.

- Légendes

  Permet d'afficher des légendes pour la voix et les sons.

Clavier

Vous pouvez effectuer les réglages suivants sur votre clavier.

- Vitesse de répétition

  Permet de définir la vitesse à laquelle un caractère se répète lorsque vous tapez sur une touche.

- Bips

  Permet d'entendre des bips lorsque vous appuyez sur certaines touches.

- Touches rémanentes

  Cette option permet aux utilisateurs tapant avec une main ou un doigt de choisir d'autres configurations du clavier.

Raccourcis clavier

Le tableau suivant répertorie les raccourcis clavier pris en charge par CA Client Automation :

Clavier	**Description**
Ctrl + X	couper
Ctrl + C	copier
Ctrl + K	Rechercher suivant
Ctrl + F	Rechercher et remplacer
Ctrl + V	coller
Ctrl + S	Enregistrer
Ctrl + Maj + S	Tout enregistrer
Ctrl + D	Supprimer la ligne
Ctrl + Flèche droite	Mot suivant
Ctrl + Flèche vers le bas	Défilement de la ligne vers le bas
Fin	Fin de ligne

Remarque : La touche d'accès rapide F6 a été ajoutée dans ce Feature Pack afin d'améliorer l'accessibilité du produit. La touche F6 simplifie la navigation entre les volets du catalogue Software Delivery et de la visionneuse Remote Control.

Souris

Vous pouvez utiliser les options suivantes pour optimiser l'utilisation et la vitesse de votre souris.

- Vitesse de clic

  Permet de choisir la vitesse du clic de souris lors d'une sélection.

- Verrouillage de clic

  Permet de mettre en surbrillance ou de faire glisser des éléments en maintenant le bouton de la souris enfoncé.

- Action inverse

  Permet d'inverser les fonctions contrôlées par les boutons gauche et droit de la souris.

- Fréquence de clignotement

  Permet de choisir la vitesse de clignotement du curseur et s'il doit clignoter ou pas.

- Options de pointeur

  Permet d'effectuer les actions suivantes :

  - Masquer le pointeur pendant la saisie
  - Afficher l'emplacement du pointeur
  - Définir la vitesse de déplacement du pointeur à l'écran
  - Sélectionner la taille et la couleur du pointeur pour bénéficier d'une visibilité accrue
  - Déplacer le pointeur vers un emplacement par défaut dans une boîte de dialogue

Annexe J: Texte tronqué dans la visionneuse Remote Control

La définition des paramètres d'affichage sur Contraste élevé dans la visionneuse Remote Control peut entraîner la troncation du texte. Un texte de remplacement permet de résoudre ce problème.

Annexe K: Modification possible du contenu de la liste des liens en fonction de la sélection effectuée

Lorsque vous appuyez sur les touches Inser + F7, certains liens n'apparaissent pas dans la fenêtre de liste des liens de la visionneuse Remote Control. Le contenu des listes de liens peut changer en fonction de votre sélection, car il existe deux vues HTML sur la page de la visionneuse Remote Control.

Les liens de la vue HTML sélectionnée s'affichent dans la fenêtre de liste des liens. Vous pouvez utiliser la touche d'accès rapide F6 pour passer d'une vue HMTL à une autre. Cette touche s'avère utile pour lire les informations affichées dans la fenêtre du lecteur d'écran, car le lecteur d'écran se comporte différemment en fonction de la vue HTML sélectionnée. La page de la visionneuse Remote Control inclut deux vues HTML, mais le lecteur d'écran lit la vue HTML sélectionnée.

Annexe L: Utilisation du lecteur d'écran JAWS dans la visionneuse et dans le module de relecture Remote Control

Le logiciel de lecture d'écran de JAWS® ne parvient pas à lire les fenêtres comprenant plusieurs affichages HTML. Il s'agit d'un problème connu. Après une utilisation prolongée, la navigation à l'aide du clavier et l'activation des liens peuvent devenir imprévisibles.

Pour obtenir de meilleures performances, nous vous recommandons de désactiver l'option Sous forme de page Web dans le menu Vue actuelle de la visionneuse ou du module de relecture Remote Control. Vous pouvez également masquer la barre de didacticiel si vous ne l'utilisez pas.

Pour de meilleurs résultats d'affichage dans la visionneuse Remote Control, vous pouvez également désactiver le curseur de PC virtuel à l'aide de la combinaison de touches JAWS + Z.

Annexe M: Restrictions liées aux sessions distantes

Le lecteur d'écran et les modifications apportées aux paramètres d'affichage ne sont pas gérés par la visionneuse Remote Control pour les sessions distantes.

Annexe N: Fonctionnalités du mode de contraste élevé

En mode de contraste élevé, la visionneuse Remote Control effectue automatiquement quelques changements visuels pour améliorer la visibilité de l'interface utilisateur. Si le mode Contraste élevé est activé ou désactivé de façon dynamique lorsque la visionneuse Remote Control est en cours d'utilisation, actualisez l'interface utilisateur graphique, par exemple en basculant vers un autre noeud, afin d'afficher les modifications apportées par le mode Contraste élevé.

Remarque : Pour actualiser la page de didacticiel de la visionneuse Remote Control, vous pouvez cliquer sur l'un des liens du didacticiel.

Glossaire

Actualisation d'ordinateur

L'*actualisation d'ordinateur* est le processus de réinitialisation de l'ordinateur virtuel vers son état d'origine. Le suivi des clones liés passe à l'ordinateur virtuel contenant le clone. Pour contrôler les allocations de stockage avec le clone, VMWare View permet d'effectuer l'opération d'actualisation, qui réinitialise le clone vers sa référence et libère tous les produits delta fournis aux fins de modifications du suivi. En d'autres termes, toutes les informations stockées sur le disque système, car la création du clone ou sa dernière actualisation ou recomposition est perdue. Contrairement à une recomposition d'ordinateur, le même modèle Or est toujours utilisé tel qu'avant l'opération d'actualisation.

application

Une *application* est un composant logiciel, par exemple Microsoft Word.

Application de patchs hors ligne

L'application de patchs hors ligne vous permet d'exporter le contenu et les fichiers de patch à distance et de les importer dans l'environnement Client Automation à l'aide de CA Patch Manager, sans devoir accéder à Internet.

application provisionnée

Une *application provisionnée* est une application (standard ou virtuelle) qui est mise à disposition pour exécution sur un ordinateur cible. Il n'est pas nécessaire de l'installer localement pour pouvoir la traiter en tant qu'application provisionnée.

application standard

Une *application standard* est un logiciel d'application qui n'a pas été virtualisé est qui peut être installé et exécuté de façon traditionnelle. Il est fait référence aux applications standard lorsqu'on parle de versions, de patchs et de suites.

application virtualisée autonome

Une *application virtualisée autonome* est une application virtualisée qui a été provisionnée d'une façon telle que l'image d'application virtualisée utilisée comme source réside sur le système vers lequel l'application a été provisionnée.

application virtualisée diffusée

Une *application virtualisée diffusée* est une application virtualisée qui a été provisionnée d'une façon telle que l'image d'application virtualisée utilisée comme source réside sur un système distant qui est différent de celui vers lequel l'application a été provisionnée.

application virtuelle

Une *application virtuelle* est un logiciel qui a été virtualisé.

bac à sable

Un *bac à sable* est un environnement d'exécution d'applications qui isole une application du système d'exploitation et des ressources de l'ordinateur ainsi que des autres applications installées sur l'ordinateur. Le degré d'isolement est habituellement défini sur une valeur permettant à l'application d'accéder aux ressources du système d'exploitation, telles que le dossier des documents.

Base de données des états de logiciel d'instance

La *base de données des états de logiciel* d'instance représente une partie de la base de données des états de logiciel qui contient l'historique de tous les jobs logiciels exécutés par l'agent exécuté sur un système de modèle autre que Or, c'est-à-dire, tout clone du modèle Or.

Clones liés

Dans VMWare View, les *clones liés* d'une image principale ou Or font uniquement référence à cette dernière, mais ne l'incluent pas. Les modifications apportées au système lors des sessions d'utilisateur ne sont pas stockées dans l'image principale, mais sont conservées dans des fichiers de différences avec le clone.

Clones non liés

Dans VMWare View, *les clones liés,* ou clones complets, sont les copies complètes d'une image principale ou Or. Le clone inclut une copie de l'image et toutes les modifications apportées au système lors des sessions d'utilisateur y sont stockées.

Clones non persistants

Les clones non persistants sont des ordinateurs virtuels du pool non persistant de données de l'utilisateur VMWare View qui sont transitoires préconfigurées. Lors de la déconnexion d'un utilisateur, le clone est actualisé et toutes les données de l'utilisateur sur le disque système sont perdues.

Clones persistants

Les clones persistants sont des ordinateurs virtuels du pool persistant qui demeurent tels quels après la déconnexion de l'utilisateur, jusqu'à leur actualisation ou recomposition. VMWare View contient des unités distinctes et préconfigurées pour le système et les données de l'utilisateur avec les clones persistants. Les informations stockées sur l'unité des données de l'utilisateur demeurent après une action d'actualisation ou de recomposition, tandis que les modifications apportées au disque système sont perdues.

cluster d'hôte

Un *cluster d'hôte* est un ensemble cumulé de ressources informatiques et de mémoire d'un groupe d'hôtes partageant l'intégralité ou une partie d'un même réseau et média de stockage.

Common Configuration Enumeration (CCE)

La norme SCAP *Common Configuration Enumeration (CCE)* contient des identificateurs standard et un dictionnaire des problèmes de configuration du système liés à la sécurité. Dans un flux de données SCAP, une définition de règle peut contenir des références à un ou plusieurs identificateurs CCE, ce qui signifie que la règle constitue une représentation des recommandations applicables aux configurations CCE ou au contrôle de configuration. Pour plus d'informations, visitez le site http://cce.mitre.org/.

Common Platform Enumeration (CPE)

La norme SCAP *Common Platform Enumeration (CPE)* contient des identificateurs standard et un dictionnaire d'attributions de noms aux produits et aux plates-formes. Par exemple, l'application de certains éléments des fichiers XCCDF peut se limiter à certaines plates-formes à l'aide d'identificateurs CPE. Pour plus d'informations, visitez le site http://cce.mitre.org/.

Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) est un dictionnaire de noms communs (ou identifiants CVE) répertoriant les vulnérabilités de sécurité des informations connues et publiques. Ces identifiants facilitent le partage des données entre différents outils et bases de données de sécurité de réseau. CVE est un des composants de SCAP. Pour plus d'informations, consultez le site http://cve.mitre.org/.

Common Vulnerability Scoring System (CVSS)

La norme SCAP *Common Vulnerability Scoring System (CVSS)* contient des normes de mesure et d'évaluation de l'impact des vulnérabilités. Pour plus d'informations, visitez le site http://www.first.org/cvss/index.html.

Connecteurs

Les *connecteurs* représentent les liens reliant des produits qui consomment des données de connecteurs à des produits externes, ou des *gestionnaires de domaines*. Chaque connecteur récupère des informations de son gestionnaire de domaines et les transmet via la structure de connecteurs vers le produit consommant aux fins de visualisation et d'analyse. Les connecteurs peuvent également effectuer des opérations entrantes sur les données du gestionnaire de domaines source, comme la création d'objet. Les connecteurs utilisent une structure de connecteurs unifiée pour activer l'intégration à plusieurs produits consommant.

Cryptographie conforme à la norme FIPS

Il est fait référence à la *cryptographie conforme à la norme FIPS* lorsque sont utilisés des modules certifiés FIPS 140-2 ainsi que des techniques et algorithmes approuvés et autorisés par la norme FIPS pour la cryptographie.

définition d'image d'application virtualisée

Une *définition d'image d'application virtualisée* est à une empreinte servant à la détection d'une image d'application virtualisée. Pour détecter une image contenant une ou plusieurs applications virtualisées incluses (stockées dedans), des signatures logicielles standard doivent être associées à la définition d'image d'application virtualisée.

disque virtuel

Un *disque virtuel* est un ensemble de fichiers qui constitue un système de fichiers qui apparaît en tant que disque physique au niveau du système d'exploitation invité.

environnement autonome

Un *environnement autonome* est un environnement dans lequel les utilisateurs des ordinateurs hôte et de la visionneuse gèrent les paramètres, propriétés et octrois de licence du composant de contrôle à distance Client Automation localement. Il est défini par l'installation d'un agent autonome. Pour une installation manuelle, le programme d'installation de l'agent RC doit être appelé directement.

Environnement d'un hôte géré de manière centralisée

Un *environnement hôte géré de manière centralisée* est un environnement où un gestionnaire d'entreprise ou de domaines de contrôle à distance est chargé de la configuration des hôtes et de l'authentification des connexions de la visionneuse. Il gère également le carnet d'adresses utilisé par les utilisateurs pour rechercher les hôtes.

Environnement géré de manière centralisée

Un *environnement géré de manière centralisée* est un environnement où le gestionnaire de domaines de contrôle à distance contrôle les paramètres de l'hôte via des stratégies d'ordinateur, des éléments du carnet d'adresses global (CAG), la licence de l'agent hôte pour le domaine et les autorisations utilisateur. Il s'agit de la valeur par défaut pour CA Client Automation.

environnement virtuel hébergé

Un *environnement virtuel hébergé* est un logiciel de virtualisation dont l'exécution est prioritaire à celle d'un système d'exploitation hôte, c'est-à-dire, d'un ordinateur physique, d'un système d'exploitation hôte et d'un hyperviseur.

environnement virtuel natif

Un *environnement virtuel natif* est un logiciel de virtualisation qui s'exécute directement sur l'ordinateur physique, et se transforme en système d'exploitation hôte (souvent minimal), c'est-à-dire, en ordinateur physique ou en hyperviseur, ou se comporte comme tel. "Environnement à chaud" est un synonyme de ce terme.

environnement virtuel partitionné

Un *environnement virtuel partitionné* est un environnement dans lequel plusieurs instances du système d'exploitation hôte peuvent s'exécuter de façon indépendante sur le même ordinateur physique. Il ne s'agit pas à strictement parler d'une technologie de virtualisation, mais l'environnement virtuel partitionné est utilisé pour résoudre le même type de problèmes.

Federal Information Processing Standard (FIPS)

FIPS (Federal Information Processing Standard) est une norme de sécurité qui est émise et approuvée par l'institut NIST. Elle indique les conditions de sécurité qui doivent être remplies par un module cryptographique utilisé dans un système de sécurité protégeant des informations sensibles, mais non classifiées.

FIPS uniquement

En mode de fonctionnement *FIPS uniquement*, seule la cryptographie conforme à la norme FIPS est autorisée. Dans ce mode, Client Automation n'est pas rétrocompatible avec les versions précédentes de Client Automation.

Flux de données SCAP

Le flux de données SCAP consiste en des données de liste de contrôle de sécurité représenté aux formats XML automatisés, énumérations relatives au nom de produit et mappages entre les énumérations. Un flux de données SCAP comprend les fichiers XML suivants :

- Un fichier XCCDF
- Un ou plusieurs fichiers OVAL
- (Optionnel) un fichier de dictionnaire CPE

format de package

Le *format de package* est une propriété d'un package logiciel. Les formats sont : standard et virtuel.

Format extensible de description de la liste de contrôle de configuration (XCCDF)

Le langage de spécification *eXtensible Configuration Checklist Description Format (XCCDF)* s'utilise pour écrire des listes de contrôle de sécurité, des bancs d'essai et d'autres types de documents connexes. Un document XCCDF constitue une collecte structurée de règles de configuration de la sécurité pour certains ensembles d'ordinateurs cibles. La spécification est conçue pour prendre en charge l'échange d'information, la génération de documents, l'adaptation organisationnelle et situationnelle, les tests de conformité automatisés et l'évaluation de la conformité. Pour plus d'informations, visitez le site http://nvd.nist.gov/xccdf.cfm.

hôte

Un *hôte*, dans la terminologie générale de virtualisation de plates-formes, est un ordinateur physique, un système d'exploitation hôte ou un hyperviseur.

hyperviseur

Un *hyperviseur* est une couche de logiciel de virtualisation qui simule le matériel physique au nom du système d'exploitation invité. Ce terme est un synonyme du terme moniteur d'ordinateurs virtuels.

image d'application virtualisée

Une *image d'application virtualisée* contient une ou plusieurs applications virtualisées stockées dans un fichier et est éventuellement accompagnée d'un ensemble de fichiers de métadonnées la prenant en charge.

image d'application virtualisée stockée sur un média intermédiaire

Une *image d'application virtualisée stockée sur un média intermédiaire* est une image d'application virtualisée qui a été détectée dans le système de fichiers d'un ordinateur.

image diffusée d'application virtualisée

Une *image diffusée d'application virtualisée* est une image d'application virtualisée qui a été détectée comme étant accessible via le réseau d'un ordinateur. En principe, la détection d'images diffusées d'application virtualisée est possible uniquement si les applications virtualisées résidant dans l'image ont été provisionnées.

image virtuelle

A *image virtuelle* est un fichier ou un ensemble de fichiers contenant l'intégralité de la définition d'un ordinateur virtuel, y compris ses spécifications au niveau du matériel et ses disques virtuels. Il s'agit de la représentation du système de fichiers de l'hôte d'un invité. Une image virtuelle peut être en ligne ou hors ligne, selon l'état d'exécution de l'ordinateur virtuel qu'elle capture.

Indicateur d'emplacement

L'indicateur d'emplacement permet à l'agent DSM d'un ordinateur de détecter l'emplacement de celui-ci.

invité

Un *invité*, dans la terminologie générale de virtualisation de plates-formes est un ordinateur virtuel et un système d'exploitation invité.

mappage de schéma

Un *mappage de schéma* est un mappage entre des noms d'attributs associés aux objets de données, tels que les utilisateurs, les ordinateurs et les groupes, utilisés dans un répertoire externe et ces noms d'attributs utilisés par les objets Client Automation correspondants. L'ensemble fixe et standard de noms d'attributs DSM est utilisé afin d'effectuer des requêtes sur les répertoires et de formuler des rapports et des requêtes complexes.

MITRE

La *MITRE Corporation* est une organisation à but non lucratif créée pour agir dans l'intérêt public. MITRE propose des interpréteurs, des codes sources, des schémas et des fichiers de données gratuits qui peuvent servir de base aux particuliers et aux organisations. Ovaldi est un exemple d'interpréteur gratuitement disponible.

Modèle Or

Dans la terminologie de Client Automation, le *modèle Or* est l'ordinateur virtuel à partir duquel les ordinateurs virtuels sont clonés.

module de cryptographie certifié FIP

Le *module de cryptographie certifié FIPS* est un module RSA CryptoC BSAFE, certifié FIPS 140-2.

National Institute of Standards and Technology (NIST)

La *National Institute of Standards and Technology (NIST)* est une agence fédérale non réglementaire du Ministère du Commerce des Etats-Unis. La mission du NIST consiste à promouvoir l'innovation et la compétitivité des industries en favorisant la science des mesures, les normes et la technologie de manière à améliorer la sécurité économique et notre qualité de vie. La National Vulnerability Database (Base de données nationale des vulnérabilités, NVD) des Etats-Unis, opérée par le NIST, fournit un référentiel et des flux de données de contenu qui utilisent les normes SCAP. Il s'agit également du référentiel de certaines données de normes SCAP officielles. Ainsi, le NIST définit des normes ouvertes dans le contexte de SCAP et définit les mappages entre les normes d'énumération SCAP.

Open Vulnerability and Assessment Language (OVAL)

La norme *Open Vulnerability and Assessment Language (OVAL)* contient des XML standards pour tester les procédures de sécurité liés à des défaillances logicielles, des problèmes de configuration et des patchs, ainsi que pour générer des rapports de résultats des tests. Toutes les vérifications de règles dans les listes de contrôle se présentent sous la forme de références de définitions OVAL dans le flux de données SCAP. Pour plus d'informations, visitez le site http://oval.mitre.org/.

ordinateur virtuel

Un *ordinateur virtuel* est un environnement virtualisé isolé qui simule un ordinateur physique. Par définition, l'ordinateur virtuel n'inclut pas le système d'exploitation invité.

Ordinateur virtuel de clone lié non persistant

Un *ordinateur virtuel de clone lié non persistant* est un ordinateur virtuel actualisé ou recomposé à chaque connexion d'utilisateur, sans persistance d'applications installées personnalisées, personnalisation, etc.

Ordinateur virtuel de clone lié persistant

Un *ordinateur virtuel de clone lié persistant* est un ordinateur virtuel dédié à un utilisateur spécifique, qui peut demander d'ajouter un logiciel particulier, de personnaliser des paramètres, etc. Lors de chaque connexion, l'environnement personnalisé de l'utilisateur est restauré. Cela persiste jusqu'à l'actualisation ou la recomposition de l'ordinateur virtuel. A ce stade, tous les produits logiciels installés sur le lecteur de système sont perdus.

Ordinateur virtuel de clone non lié persistant

Un *ordinateur virtuel de clone non lié persistant* est un ordinateur virtuel dédié à un utilisateur spécifique et lui est présenté lors de chaque connexion avec ses applications installées personnalisées, ses paramètres d'utilisateur, ses données, etc.

Ovaldi

Ovaldi est un interpréteur OVAL développé par la MITRE Corporation. Il s'agit d'une implémentation de références disponibles gratuitement, créée pour indiquer comment les informations peuvent être collectées d'un ordinateur pour être testées en vue d'évaluer et d'exécuter les définitions OVAL pour cette plate-forme ainsi que générer des rapports de résultats des tests. L'interpréteur démontre la convivialité des définitions OVAL et garantit une syntaxe correcte et l'adhésion aux schémas OVAL.

package autonome d'application virtualisée

Un *package autonome d'application virtualisée* est un package d'application virtualisée utilisé pour ajouter une application virtualisée en mode autonome.

Package d'application virtualisée

Un *package d'application virtualisée* est une image d'application virtualisée inclue dans un ou plusieurs packages Software Delivery. Ces packages sont utilisés pour ajouter des applications virtualisées sur des ordinateurs.

package de stockage intermédiaire d'application virtualisée

Un *package de stockage intermédiaire d'application virtualisée* est un package d'application virtualisée utilisé pour le stockage intermédiaire de l'image d'application virtualisée.

package diffusé d'application virtualisée

Un *package diffusé d'application virtualisée* est un package d'application virtualisée utilisé pour ajouter une application virtualisée en mode diffusion.

partition

Une *partition* est une instance individuelle d'un système d'exploitation hôte. En principe, les partitions n'utilisent pas de systèmes d'exploitation invités parce qu'ils partagent tous le système d'exploitation de l'hôte.

patch virtuel

Un *patch virtuel* est l'équivalent virtuel d'un patch standard, avec une utilité fondamentalement identique. Le terme est utilisé lors de la génération de rapports d'inventaire des logiciels pour les applications virtualisées (pas pour les images d'application virtualisée).

Préférence FIPS

En mode de fonctionnement *Préférence FIPS*, toutes les opérations cryptographiques sont conformes à la norme-FIPS, c'est pourquoi peu de chiffrements conservent le format hérité. Dans ce mode, Client Automation n'est pas-rétrocompatible avec les versions précédentes de Client Automation.

Profil XCCDF

Un *profil XCCDF* est une stratégie appliquée à l'ordinateur cible ou comparée à la configuration de cet ordinateur cible. Le fichier XCCDF de chaque flux de données SCAP définit la liste de profils pris en charge. Le fichier XCCDF doit avoir au moins un profil XCCDF, qui spécifie les règles à utiliser pour vérifier un type particulier de système. Vous pouvez créer des profils XCCDF distincts pour chaque environnement opérationnel applicable dans lequel un système peut être déployé.

Recomposition d'ordinateur

La *recomposition d'ordinateur* est le processus d'affectation d'un nouveau modèle Or à l'ordinateur virtuel. Les systèmes d'exploitation et les applications doivent être gérés pendant leur durée de vie afin de corriger des problèmes résolus par des correctifs ou des services packs, ou de fournir de nouvelles fonctionnalités via de nouvelles versions. Dans le cas de clones liés, cela signifie que l'image principale, ou le modèle Or, doit être mis à jour. Une fois que les mises à jour sont terminées, le clone lié est recomposé et devient actif. Pendant l'opération de recomposition, les clones liés sont connectés à ce nouveau modèle Or et actualisés.

Réinstallation hors ligne après un arrêt brutal

La réinstallation hors ligne après un arrêt brutal est une tâche de réinstallation après l'arrêt brutal (RAC) effectuée par l'agent plutôt que par le gestionnaire. Les ordinateurs virtuels sont *recomposés* fréquemment, à savoir, chaque fois que le modèle Or est mis à jour et le disque réinitialisé ; toute modification apportée à l'ordinateur virtuel par rapport à la réinitialisation précédente est efficacement évitée. Dans le cas d'ordinateurs virtuels, l'agent (non le gestionnaire) est responsable de la création du conteneur de jobs RAC. Lors de la réinitialisation du disque, l'agent initialise une réinstallation hors ligne après un arrêt brutal pour restaurer tout logiciel déployé vers l'agent.

Réplication

La *réplication* est une tâche de moteur permettant d'effectuer la réplication des données du gestionnaire de domaines vers le gestionnaire d'entreprise et du gestionnaire d'entreprise vers le gestionnaire de domaines.

Security Content Automation Protocol (SCAP)

Le protocole *Security Content Automation Protocol (SCAP)*, est une méthode d'utilisation des normes telles que XCCDF, CCE, CVE, CVSS, CPE, et OVAL dans le cadre de l'évaluation automatisée de la conformité aux stratégies, aux mesures et de la gestion de la vulnérabilité (par ex. conformité FISMA). Plus particulièrement, SCAP est une suite de normes ouvertes sélectionnées qui énumèrent les défaillances logicielles, les problèmes de configuration liés à la sécurité et les noms de produit, de systèmes de mesure pour déterminer la présence de vulnérabilités et fournissent des mécanismes pour classer (évaluer) les résultats de ces mesures afin d'évaluer l'impact des problèmes de sécurité rencontrés. SCAP définit comment ces normes sont combinées. La National Vulnerability Database fournit un référentiel et des flux de données de contenu utilisant les normes SCAP. Pour plus d'informations, visitez le site http://nvd.nist.gov/xccdf.cfm.

serveur de modularité

Un *serveur de modularité* est un serveur central qui permet de moduler les tâches de gestion. Il s'agit d'un processus réparti constituant l'interface principale pour l'agent.

signature logicielle

Une *signature logicielle* définit les attributs d'un logiciel, tels que le nom du fichier exécutable principal, les autres fichiers associés, la plage de taille, la plage de version, ainsi que les dates de création et de modification du logiciel. Tous ces attributs d'une signature logicielle identifient de manière unique une application logicielle. Les signatures logicielles d'Asset Management sont créées comme des définitions logicielles. Vous pouvez créer des définitions de logiciels pour un produit, une version, un patch, une suite, le composant d'une suite ou l'image d'une application virtualisée. Par défaut, Asset Management fournit des signatures logicielles prédéfinies couvrant les logiciels les plus utilisés dans le secteur informatique.

Surveillance de l'intégrité

La fonctionnalité de *surveillance de l'intégrité* vous permet de configurer des alertes, de définir des seuils et de surveiller l'intégrité globale de l'infrastructure Client Automation.

système d’exploitation hôte

Un *système d'exploitation hôte* est un système d'exploitation en cours d'exécution sur un ordinateur physique.

système d’exploitation invité

Un *système d'exploitation invité* est un système d'exploitation en cours d'exécution sur un ordinateur virtuel.

type de logiciel

Le *type de logiciel* est une propriété d'une définition de logiciel. Types actuels de logiciels : suite, produit, version, patch et image d'application virtualisée.

type de package

Le *type de package* est une propriété d'un package logiciel. Les types actuels sont : Générique, MSI, SXP, PIF et PKG. Le type de package n'est pas utilisé ou altéré dans le cadre de la prise en charge des packages d'application virtualisée.

Unité cible principale

Dans Citrix XenDesktop, une *unité cible principale* est l'ordinateur de base sur lequel est installé le système d'exploitation et l'ensemble d'applications requis à partir desquelles un vDisk est généré.

vDisk

Dans Citrix XenDesktop, un *vDisk*, ou disque virtuel, est un simple fichier image contenant le système d'exploitation et l'ensemble requis d'applications.

vDisk principal

Dans Citrix XenDesktop, un *vDisk principal* est le vDisk initial généré à partir de l'ordinateur de modèle Or.

version virtuelle

Une *version virtuelle* est l'équivalent virtuel d'une mise en production standard, avec une utilité fondamentalement identique. Le terme est utilisé lors de la génération de rapports d'inventaire des logiciels pour les applications virtualisées (pas pour les images d'application virtualisée). Les applications virtualisées provisionnées peuvent utiliser une image d'application virtualisée diffusée en continu ou stockée sur un média intermédiaire en tant que source. Les applications virtualisées contenues dans l'image d'application virtualisée peuvent apparaître comme stockées sur un média intermédiaire, mais comme n'ayant pas encore été provisionnées.

virtualisation d'application

La *virtualisation d'application* est l'encapsulation d'une application, qui est séparée du système d'exploitation sous-jacent sur lequel elle est exécutée. Lors de l'exécution, l'application accepte d'agir comme si elle communiquait directement avec le système d'exploitation d'origine et toutes les ressources gérées par celui-ci, alors qu'en réalité une telle communication n'a pas lieu.

virtualisation de la plate-forme

La *virtualisation de la plate-forme* est l'encapsulation d'ordinateurs ou de systèmes d'exploitation, qui ne mettent pas leurs caractéristiques physiques à disposition des utilisateurs et qui émulent la plate-forme informatique lors de leur exécution.

vue de configuration

Une *vue de configuration* est une interface utilisateur Windows personnalisée qui vous permet de modifier les stratégies de configuration liées aux composants ou aux fonctionnalités spécifiques. Les vues de configuration résument les stratégies utiles pour un composant ou une fonctionnalité sans tenir compte de l'endroit où ils se situent dans la hiérarchie et l'arborescence de l'explorateur DSM.